

# GAPCO

## TRADE & COMMUNICATIONS SURVEILLANCE:

---

### APPROACHES TO VENDOR SELECTION



|   |           |
|---|-----------|
| <b>Contents</b> .....   | <b>2</b>  |
| <b>Introduction</b> .....   | <b>3</b>  |
| Surveillance today .....  | 3         |
| Vendor selection.....   | 4         |
| How this report can help you.....                                 | 5         |
| Acknowledgements .....  | 5         |
| <b>1. Drivers and trends impacting surveillance in 2023</b> ..... | <b>6</b>  |
| <b>1.1 Market drivers</b> .....                                   | <b>7</b>  |
| Market volatility.....  | 7         |
| Home working.....   | 8         |
| <b>1.2 Regulatory drivers</b> .....                               | <b>9</b>  |
| Enforcement activity .....  | 9         |
| Supervisory technology.....                                       | 11        |
| Regulatory trends .....   | 11        |
| <b>1.3 Solution trends</b> .....                                  | <b>12</b> |
| Holistic surveillance .....                                       | 12        |
| Machine learning, AI and NLP.....                                 | 13        |
| Cloud adoption .....  | 14        |
| <b>2. Solution selection criteria and dependencies</b> .....      | <b>15</b> |
| Buy versus build.....   | 15        |
| Vendor landscape.....   | 15        |
| <b>2.1 Target client and alerting</b> .....                       | <b>17</b> |
| Target client.....  | 17        |
| Alerting, calibration and minimising false positives.....         | 18        |
| Asset class .....   | 19        |
| Machine learning and analytics .....                              | 20        |
| <b>2.2 Holistic surveillance</b> .....                            | <b>20</b> |
| Data .....  | 20        |
| Holistic surveillance .....                                       | 21        |
| Communications surveillance.....                                  | 22        |
| Market data and news provision .....                              | 24        |
| Cloud.....  | 24        |
| <b>2.3 Pricing</b> .....  | <b>25</b> |
| <b>2.4 Other factors</b> .....                                    | <b>26</b> |
| Case management .....   | 26        |
| Other use cases for surveillance tools.....                       | 28        |
| <b>Closing thoughts</b> .....                                     | <b>28</b> |
| <b>References</b> .....   | <b>29</b> |

## Surveillance today

Clean markets are essential for everyone. Market abuse scandals – whether the Wall Street insider trading scandals of the 1980s, IBOR and FX benchmark rigging in the early 2010s, or the fall-out from the crypto exchange implosions in 2022 – undermine not just the reputation and bottom lines of the firms involved but impact the strength of the overall market system. For that reason, surveillance remains vitally important and a top priority of not just the UK's Financial Conduct Authority (FCA) but also its regulatory counterparts in the US, Canada, Europe and, increasingly, in emerging market economies.

Banks have made significant progress during the last decade in better managing market abuse risk. This progress is, in large part, due to the significant supervisory burden placed on firms by the wave of regulations introduced following the 2008 financial crisis – with Dodd Frank, MAR and MiFID II requiring a level of monitoring not seen before. And regulators are continuing to step up their enforcement efforts, whether through investments in supervisory technology, clamping down on unsupervised communications channels (as per the record circa \$1.8bn WhatsApp fines levied in the US by the SEC and CFTC in 2022), the roll out of new market cleanliness measures such as the FCA's Potentially Anomalous Trading Ratio (PATR) in 2018, and the continued evolution of market abuse law and guidance (e.g. the legality of shadow trading, and 10b5-1 schemes).

Bad actors will never entirely disappear, and they continue to evolve their approaches in an attempt to fly under the radar of surveillance systems. Indeed, the FCA's PATR found that in 2021, 6.1% of trades during price sensitive announcements were anomalous; and the move to hybrid working also presents new challenges in monitoring the dissemination of inside information. At the same time, in addition to the classic market abuse behaviours (e.g. insider trading, layering/spoofing, wash

trades, marking the close/open), newer forms are emerging – these include pump and dump schemes led by social media 'finfluencers' and cybersecurity events (e.g. the hacking of regulator or newswire press releases prior to their publication to enable insider trading, and the dissemination and sale of confidential company information on the dark web).

A typical bank analyses between one million and three million trade and comms alerts per year (an average of 3,000-10,000 alerts per day<sup>1</sup>). For each Suspicious Transaction Order Report (STOR) a bank raises, it will review anywhere from 15,000-45,000 alerts, a vivid demonstration of the scale of false positives and potential to optimise alerting through effective alert calibration and analytics technologies. To manage these high caseloads, banks have employed hundreds of on- and off-shore analysts – resulting in average annual surveillance spends, across technology and staff, of \$10 million to \$50 million per year. And despite this sizeable spend, instances of market abuse still slip through the net, only to be detected when the regulator comes knocking.

So whilst surveillance is not a profit-making activity, and today's financial climate is very much focussed on cost-cutting, firms must exercise due caution in reducing investment levels. Safe, trusted and compliant business encourages investment and attracts clients; the obverse can lead to regulatory enforcement actions with huge penalties and negative publicity. Firms can, however, still optimise their surveillance frameworks, without massively increasing investment levels. For example, through building well-tailored risk assessments, designing an efficient operating model, effectively defining your surveillance tool requirements and making well-informed vendor solution decisions.

## Vendor selection

Given the size of the fragmented surveillance market – with up to 30 leading vendors and the complexity of surveillance systems – it is not easy to navigate the market and select the right system to meet your unique needs.

### Key considerations include:

**Functionality choices** – the large number of players brings with it a daunting array of functionality choices, including:

- **Scope of solution** – holistic or trade/comms specific solutions; broader financial crime and compliance offerings or surveillance only solutions
- **Technology** – analytics technologies including machine learning, or traditional rules based models; cloud or on premises delivery; T+1 or real-time monitoring
- **Data** – volumes of trades and orders that can be processed; vendor or customer-managed data normalisation; whether your solution provides market data (and if so which data provider)
- **Alert calibration** – vendor-led or self-calibrated algorithms (and self-calibration via programming languages or intuitive drop down options)
- **Communication surveillance** – whether the provider simply monitors communications or also ingests and archives the communications; the number of communication channels ingested; smart or standard lexicons
- **Other** – the ease of the user interface and practicality of trade replay visualisations; the quality and speed of customer service; some firms even offer managed services acting as a first line filter for alert reviews.

**FICC coverage:** Management of the trade surveillance risks associated with FICC (Fixed Income, FX and Commodities) is an area of increasing regulatory scrutiny, given the challenges

associated with obtaining relevant data for OTC trades, recording RFQ data, and questions of how best to assess possible manipulation (e.g. whether through price or yield changes). Providers are upgrading their solutions to meet this challenge.

**Consolidating solution stack:** Firms can consolidate their solution stack, both within surveillance itself (some large banks operate 10+ separate solutions) as well as across associated functions to achieve cost and operational efficiencies. For example, rather than operating separate HR and Trade communications solutions, a single solution can be utilised with multiple lexica to differentiate between respective use cases. With many banks implementing new communications surveillance solutions to ensure adherence to the recent UK Consumer Duty regulation, this presents an additional opportunity to adopt a holistic approach.

**Communications surveillance:** The most cutting-edge communications surveillance providers utilise smart lexicons and NLP – for example, applying alerts to entire sentences rather than single words or phrases (e.g. “I’ll message you on WhatsApp to discuss my birthday plans” would not be flagged through this approach); this has been shown to reduce false positive rates by as much as 10-20 times. Additionally, advanced voice communications technologies are achieving transcription accuracy rates of over 90%.

**Smaller firms upgrading in-house or manual solutions:** With the regulatory radar increasingly turning to smaller firms and those catering to retail customers, this is a good time for relevant buy-side and trading firms to upgrade their in-house or manual solutions. FCA Marketwatch 73 (April 2023), with its focus on the adequacy of surveillance frameworks across brokers offering CFD (contract for difference) and spreadbet products, suggests such firms will be increasingly scrutinised going forward.

## How this report can help you

This comprehensive report, the first of its kind in more than five years,<sup>2</sup> aims to assist surveillance, compliance and banking professionals in navigating the surveillance vendor market. It is based on in-depth demos and follow-ups with 20 leading vendors, as well as extensive side of desk research of over 100 sources (including regulatory newsletters, consultancy and market reports, and vendor materials).

The report is structured as follows: Chapter 1 provides an overview of trends in today's surveillance landscape; Chapter 2 moves on to outline in detail the key selection criteria (and

dependencies) to consider when selecting a solution; and the Addendum – available on request – offers a summary of each vendor solution.

We encourage market participants to use this paper to enhance their knowledge of the surveillance vendor market, and aid in shortlisting suitable vendors. If you are interested in further support with vendor selection, solution implementation or evaluating your organisation's current surveillance capabilities, please reach out to Capco.

## Acknowledgements

We wish to thank the below surveillance solution providers for their time and valuable insights.




- ACA Group (Compliance Alpha)
- Behavox (Quantum AI)
- B-next (CMC eSuite)
- Broadridge
- Eventus (Validus)
- FIS (Market Surveillance Manager)
- Kx Systems (Kx for Surveillance)
- Kaizen Reporting
- Nasdaq SMARTS (Trade Surveillance; Market Surveillance)
- NICE Actimize (SURVEIL-X; NTR-X)
- OneTick (OneTick Trade Surveillance)
- Scila (Scila Surveillance)
- Software AG (Apama)
- Solidus Labs (HALO)
- SteelEye
- SymphonyAI (Sensa-NetReveal)
- Trading Technologies (TT Score)
- Trading Hub (MAST; CaaS)
- Trillium (Surveyor)
- VoxSmart

# DRIVERS AND TRENDS IMPACTING SURVEILLANCE IN 2023

Market and regulatory drivers – including home working, trading volatility, and increased regulatory enforcement and scrutiny have led to increased surveillance alerting volumes. To keep pace with the increasing demands, financial institutions (FIs) and surveillance vendors have upgraded solutions and processes – including exploring holistic surveillance approaches, increased usage of AI/machine learning (ML) and cloud adoption.

We expand on the above across the following pages.

## Macro-drivers and trends in today’s surveillance solutions

| 1 MARKET DRIVERS    | 2 REG DRIVERS   | 3 SOLUTION TRENDS   |
|--|--|--|
| <p><b>Market activity / volatility:</b> Trading volumes have grown significantly since 2020 as well as marked increase in market volatility leading to increased false positives</p> <p><b>Home working:</b> Increased complexity in detecting market abuse; greater temptation and opportunity for market abuse</p> | <p><b>Record enforcement levels:</b> US market abuse fines totalled circa \$4.2bn (2020-2022)</p> <p><b>Supervisory technology:</b> Continued growth in vendor tool usage by regulators</p> <p><b>Other reg trends:</b></p> <ul style="list-style-type: none"><li>• New communications channels enforcement</li><li>• Growth in voice surveillance</li><li>• Growing buy side scrutiny</li><li>• Continued focus on cross product manipulation</li><li>• Regulatory focus on data quality</li><li>• Crypto surveillance</li><li>• AML and surveillance synergies</li></ul> | <p><b>Holistic surveillance:</b> Many FIs still operate 5-10+ solutions; push to consolidate and utilise integrated dashboards</p> <p><b>ML and AI:</b> Usage of supervised learning to support alert triaging and threshold calibration</p> <p><b>Cloud:</b> Push for cloud adoption driven by cost savings and ease of implementation / upgrades</p> |

Source: Capco

# 1.1 MARKET DRIVERS

## Market volatility

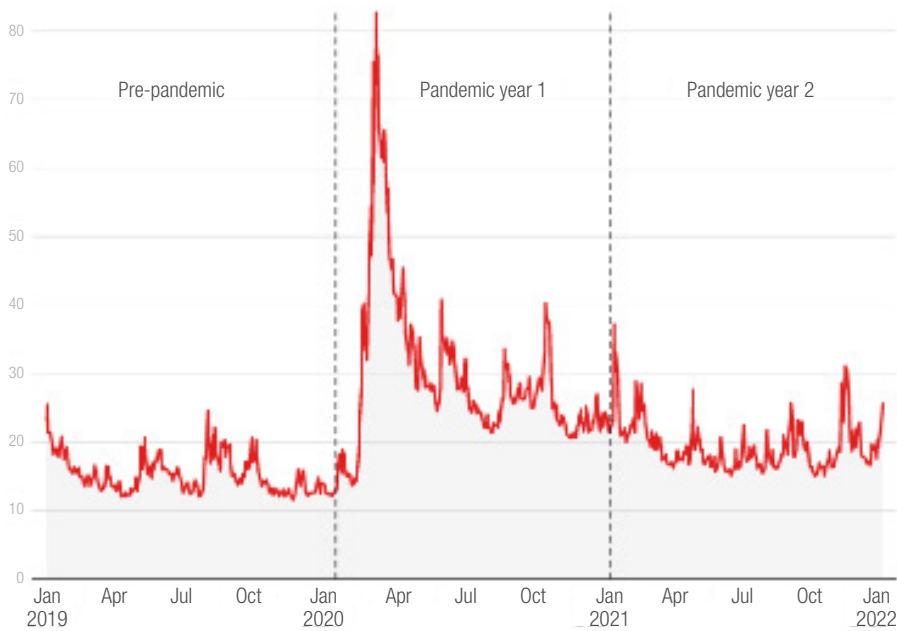
Even before the COVID pandemic, trading volumes had seen a significant increase driven through the increased electronification of trading and the growth in algorithmic trading firms.

COVID has seen trading volumes increase driven both by the increasing participation of retail investors, and significant market volatility. Per a SteelEye report “95% of all intraday price improvements greater than two standard deviations

have happened in the last 2.5 years [and] seven events where the intraday price increased by over 15 standard deviations occurred in the past year [i.e. 2022]”.<sup>3</sup>

This has caused compliance teams to spend increased time closing surveillance alerts and false positives. And whilst pandemic levels of volatility have attenuated, moderate volatility persists presenting continuing challenges to compliance teams.

Trade volatility in the US stock markets 2019-2022



Source: Cboe Volatility Index (VIX) via Yahoo Finance as per TIME Magazine

## Home working

Alongside the above market dynamics, the other major shift in the last few years has been the transition to the ‘new normal’ of home and hybrid working arrangements. This naturally heightens compliance risks – alongside the reduction in in-person office monitoring, there is an increased risk of personal

device usage, the proliferation of encrypted communication channels, and a perception of lower risk of apprehension. The worst nightmare for many compliance managers is of flatmates sharing highly sensitive information with a view to insider trading.

### Home working challenges and FI approaches

| Factor  | What firms are doing   |
|---|--|
|  <b>Personal account trading</b>                                 | <ul style="list-style-type: none"> <li>Automating personal account trading processes</li> <li>Linking personal account trading and trade surveillance systems</li> <li>Supervisory technology monitoring by regulators</li> </ul>  |
|  <b>Information leakage and insider trading</b>                | <ul style="list-style-type: none"> <li>Mandatory staff training</li> <li>Instilling culture of ethics and responsibility, led by Senior Managers</li> <li>Reviewing need to know lists</li> </ul>  |
|  <b>Unauthorised usage of personal devices</b>                 | <ul style="list-style-type: none"> <li>Updating policies and procedures</li> <li>Stopping personal devices connecting to firm networks and systems</li> <li>Controversially, at least one major financial institution updated trader contract terms to enable limited review of personal device messaging apps</li> <li>Unsupervised machine learning to detect reduced usage of work phones and emails</li> </ul> |
|  <b>Usage of unrecorded encrypted channels (e.g. WhatsApp)</b> | <ul style="list-style-type: none"> <li>Refer to page 11</li> </ul>   |



## 1.2 REGULATORY DRIVERS

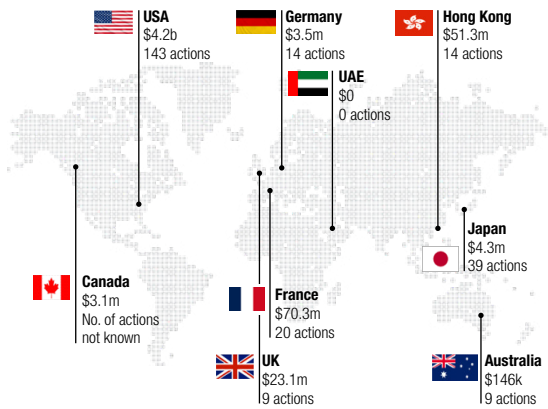
### Enforcement activity

The mood music from regulators is one of continued focus on market abuse – as articulated in public statements and expressed more overtly through investment levels and enforcement activity.

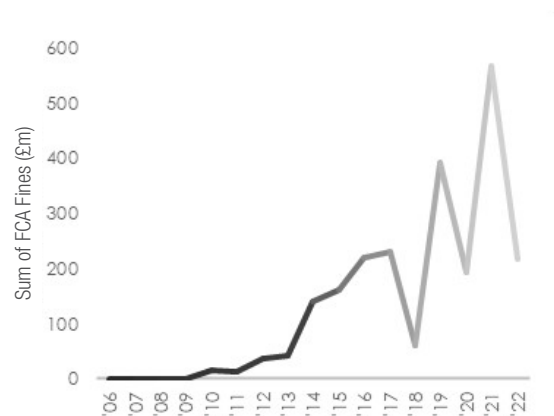
For example, the FCA announced in 2022: “Those considering attempting to manipulate our markets should be on notice that we will not hesitate to act... [to support this we draw on] the collective efforts of around 90 enforcement staff supported by dedicated specialist intelligence, legal and cyber resources as well as primary/secondary market oversight teams”. The FCA has also set up a specialist non-equity surveillance team.

Regarding enforcement activity, the SEC & CFTC continue to lead globally. In 2020-2022 their market abuse fines totalled \$1.7bn and \$2.5bn respectively across circa 140 completed actions; by comparison, France, the country with the next highest level of market abuse fines levied a total of \$70.3m across 20 completed actions. The continued strong upward trend in fines, yearly volatility notwithstanding, is reflected per the FCA chart below.

### Global market abuse fines: 2020-2022



### UK FCA market abuse and other fines: 2010-2022



**Sources:** Capco analysis of regulatory filings (including SEC, CFTC, FINRA, DoJ, CSA, FCA, AMF, BaFin, DFSA, SFC, FSA, ASIC) and press reports.

**Note:** in-scope fines include insider trading, market manipulation, communications recording issues; excluded fines include financial crime issues purely related to fraud, AML; disclosure and reporting failings; suitability, best execution, trade allocation issues. UAE’s DFSA has levied substantial AML related fines but none were identified directly related to market abuse.

Globally the market abuse focus remains on equities and fixed income (though in the US significant focus in recent years has been on commodities and FX – given the big enforcement push over the last five years by the CFTC). As regards in

scope scenarios, most actions have centred on the classic behaviours of insider trading (including tipping), front running, spoofing/layering, wash trading, pump and dump schemes and disseminating false information.

### Leading market abuse actions 2020-2022

| #  | Client  | Fine size | Year | Penalised behaviour  | Country (Regulator)  |
|----|---|-----------|------|--|--|
| 1  | 11 leading banks/brokers                                | \$1.1bn   | 2022 | Failures to preserve electronic communications (2018-2021)           | US (SEC)        |
| 2  | Leading US bank   | \$920m    | 2020 | Spoofing precious metals and US treasuries (2008-2016)               | US (CFTC)       |
| 3  | 11 leading banks/brokers                                | \$710m    | 2022 | Failures to preserve electronic communications (2018-2021)           | US (CFTC)       |
| 4  | Global commodities trading firm                         | \$485.6m  | 2022 | Manipulation of oil benchmarks and related swaps/futures (2007-2018) | US (CFTC)     |
| 5  | Multiple foreign traders                                | \$75m     | 2022 | 26 Chinese traders for spoofing 3,000+ US securities (2013-2019)     | US (SEC)      |
| 6  | Leading North American bank                             | \$60.4m   | 2020 | Spoofing precious metals (2008-2016)                                 | US (CFTC)     |
| 7  | Leading UK bank   | \$35m     | 2021 | Spoofing US Treasury securities and futures (2008-2014 and 2018)     | US (DoJ)      |
| 8  | 4 retail traders and associated companies               | \$32m     | 2020 | Pump and dump scheme involving 45+ penny stocks (2015-2019)          | US (SEC)      |
| 9  | 1 European asset manager, 1 UK broker and 2 individuals | \$40.0m   | 2021 | Futures wash trades (2014-2015)                                      | France (AMF)  |
| 10 | Leading US bank   | \$15.9m   | 2022 | Failures to properly implement MAR trade surveillance requirements   | UK (FCA)      |
| 11 | UK brokerage firm                                       | \$6.1m    | 2022 | Failures to properly implement MAR trade surveillance requirements   | UK (FCA)      |
| 12 | Private individual                                      | \$2.3m    | 2020 | Wash trades (date of offences not known)                             | Japan (FSA)   |

Source: Capco analysis of regulatory filings

## Supervisory technology

One of the most noteworthy developments in recent years has been the investment by leading regulators including in US (SEC),<sup>4</sup> UK (FCA), Canada (CSA) and APAC (JFSA and MAS) in supervisory technology to boost their monitoring capabilities. The regulators' tools run analytics on trade data submitted by firms to identify core examples of market abuse. This acts as an additional layer of checks on the surveillance work undertaken by market participants, and has had a number of resultant effects.

First, the significant investment by regulators brings with it the need to achieve results (i.e. catching and prosecuting offenders). This it demonstrably has – for example, in the US in 2021, Jose Sanchez, a compliance analyst for a leading investment bank, was prosecuted for insider trading on 45+ occasions via his parents' brokerage accounts illicitly earning \$471,000.

Moreover, that regulators are no longer solely reliant on an FI's STORs or other sources (e.g. whistle-blowers) to detect market abuse, brings with it a significant increase in compliance risk. This is an added incentive for FIs to up their game and ensure surveillance systems can detect market abuse before a regulator comes knocking on the proverbial door.

Finally, as the tools rely on FIs' transaction reporting data, this is driving increased focus by regulators on improving the quality of firms' data (and in turn on trade surveillance infrastructure). For example, FCA Market Watch 59 (April 2019) highlighted inaccuracies mapping 'short-to-long' client codes.

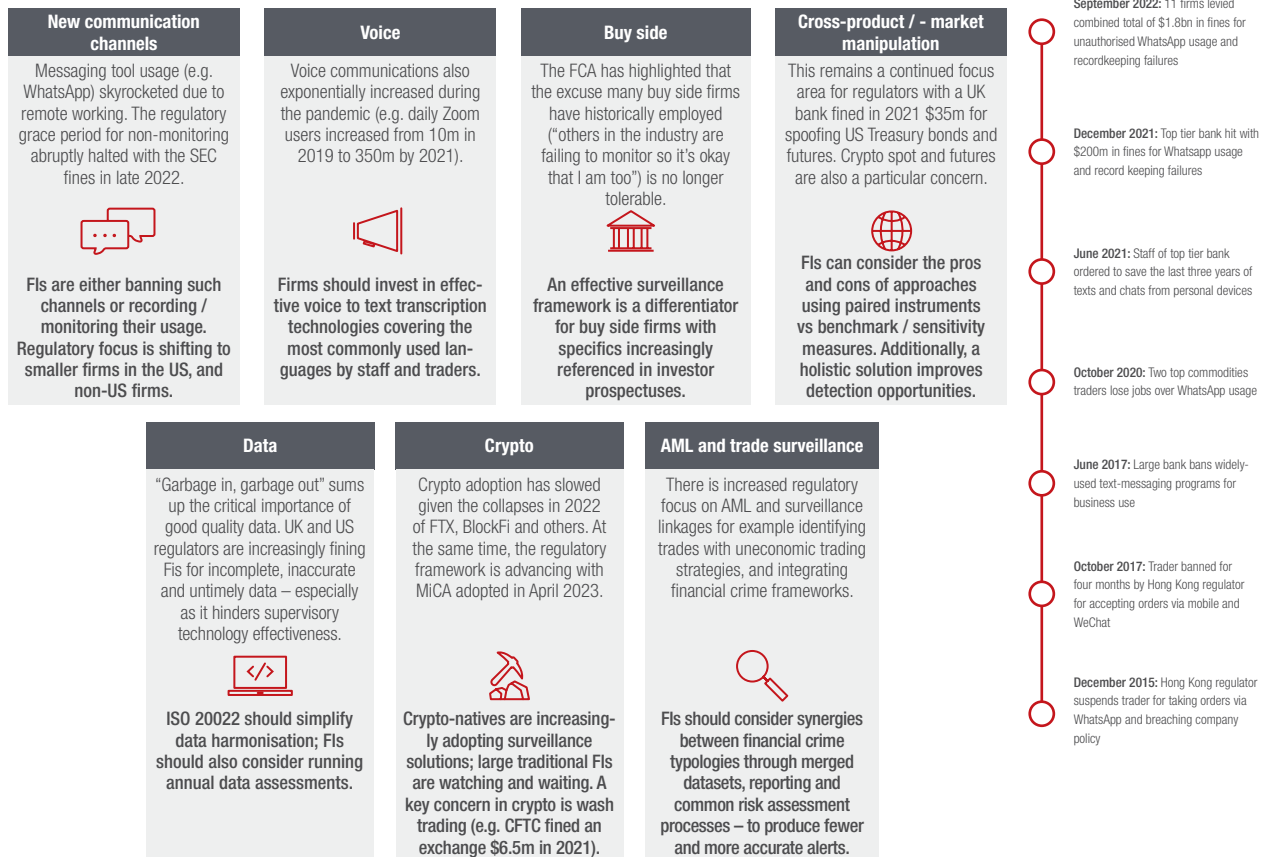
It is worth noting that whilst in the UK, for example, the regulator only analyses equities trade data; the scope is likely to expand to other asset classes in due course.

## Regulatory trends

The foremost concern for FIs in 2023 has been addressing the risk of fines for unauthorised WhatsApp communications – a regulatory issue which in fact long pre-dates 2022 (as

demonstrated in the timeline below). Additional key regulatory concern areas are noted.

### Key reg trends and timeline (till end 2022) of WhatsApp usage issues



## 1.3 SOLUTION TRENDS

### Holistic surveillance

Currently most large firms continue to operate a siloed approach to surveillance with many large financial institutions operating complex patchworks of 10+ solutions covering trade, ecomms and voice alerting. Multiple factors have contributed to this: first, the piecemeal expansion of regulatory requirements; second, the complexity of stitching together different data sets; third, a desire to utilise best in breed solutions for each asset class and communication channel; and finally, the different objectives, budgets and decision making processes across a bank.

Holistic surveillance aims to bring together disparate data sets covering trade, communication (and other key internal data such as that held in HR systems) to ensure full context is provided for each alert with a view to improving risk detection and minimising false positives. Ideally this can be achieved

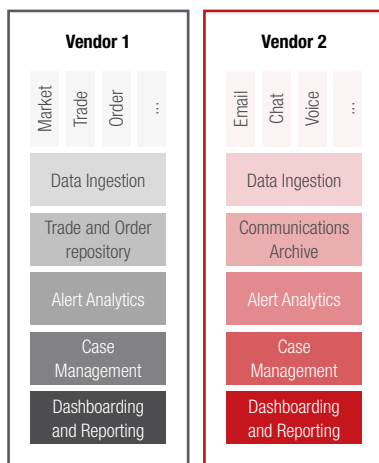
through a single main system, or otherwise a ‘holistic-lite’ or integrated approach can be achieved through having an integrated case manager to ingest alerts from the different surveillance systems.

To illustrate the benefits of a holistic approach, let’s take an example: a trader may have had an alert for wash trading. Separately, call data may show a pattern of communication with the suspected wash trading participant. HR data may additionally show this trader has had compliance issues relating to training completion. In a siloed surveillance world, each data point would tend to be viewed separately, whereas a holistic view enables a full picture to be presented in order to determine the risk and quickly determine whether the alert should be escalated, or rejected.

### Siloed, integrated and holistic surveillance approaches

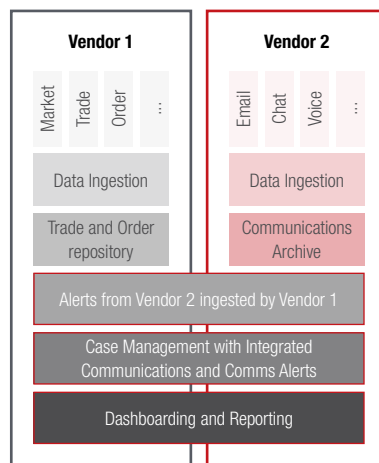
#### Siloed approach

- Using different solutions for each surveillance discipline (trade, comms etc.), where the solutions are not integrated
- **Pros:** Can select vendors based on best fit for each area; no single vendor dependency
- **Cons:** Can be expensive; no view of data across different areas



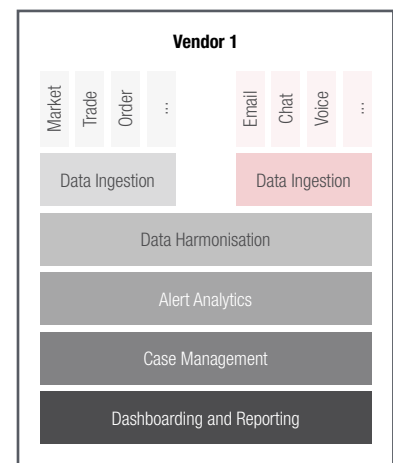
#### Integrated approach

- Using different solutions for each surveillance discipline, but the solution can ingest alerts from other systems
- **Pros:** Additional alert types from different data sets provide a more contextualised view of activity
- **Cons:** Matching can be inaccurate, limited vendor selection with offering



#### Holistic approach

- Single solution ingests data across all surveillance disciplines and harmonises data to build behavioural profiles and cross area alerting
- **Pros:** Strong data driven insights; advanced alert specificity and accuracy; efficiency
- **Cons:** Limited vendor selection; largely still in development; single vendor dependency



## Machine learning, AI and NLP

FIs rely on parameter and threshold based alert scenarios for trade surveillance (sometimes referred to as rules-based surveillance) – with updates taking place during annual calibration reviews. Frequently the settings can be under or over calibrated, either resulting in risks being missed or in large volumes of alerts and false positives – a typical bank can generate 3,000+ alerts per day with 99%+ being false positives. These issues can be particularly exacerbated during times of market stress.

Machine learning – in both its supervised and unsupervised forms – can help address the issue of missed risks and false

positives; acting as a complement to rules-based approaches. In doing so, it holds the promise of potentially reducing compliance costs.

As regards the regulatory perspective, this has evolved in recent years. With regulators' push for innovation and digital and data first solutions, they are increasingly open to new approaches for tackling market abuse. The risks of machine learning expressed by the FCA's Financial Crime Lead in 2018 regarding "simply turning an algorithm loose" has evolved to a more nuanced one, supportive of targeted usage of these technologies.

## Unsupervised machine learning

Also known as anomaly detection and behavioural analytics – unsupervised learning is used to uncover "unknown unknowns" through pattern recognition and outlier detection. Any anomalies detected are flagged for review and investigation, and serve as a separate stream of alerts to those generated via trade and comms surveillance alert scenarios. To take a few example use cases:

- Desks generating large volumes of alerts or very few could be flagged for review
- If a trader's number of emails or phone calls suddenly drops, does this indicate he/she is utilising a personal device
- Has a trader's P&L suddenly changed (and does it differ significantly from other traders on his desk) – perhaps before he was earning \$50,000 per day working in the office, and now working from home is amassing \$300,000 per day.

## Supervised machine learning

In this case, the surveillance solution progressively learns based on past alert outcomes whether an alert is likely to be a true positive or not – and ascribe either a score (0-10/0-100) or confidence level (high, medium low). This allows analysts to focus on the most high-priority alerts. Importantly, it does not result in other low(er) priority alerts being excluded.

In addition, the ML model can be used to suggest potential changes to alert scenario parameters and thresholds, which can be reviewed during quarterly or annual alert calibration re-assessments.

We have observed different approaches being used to optimise data scoring, including:

- Rather than simply closing alerts as escalate, closed, false positive etc., analysts can ascribe scores to the alert as 0-10 indicating how likely an alert is to be a true positive
- You can only focus on certain analysts (and exclude others) to build up the supervised learning data set
- Reports and dashboards can measure the accuracy of the supervised learning data set and model(s)
- Some vendors offer partner FIs to crowdsource supervised learning data sets to reduce the time taken to build up relevant size data sets (of 10,000-100,000+ alerts).

## Cloud adoption




The financial services industry was initially slow to adopt cloud technologies, but in recent years cloud adoption has grown dramatically across financial services, including with surveillance solutions.

Key drivers for this have been increased surveillance costs, the increased voice and ecomms data storage requirements, and a desire to therefore achieve cost savings. For example, NICE Actimize has referred to “several large Tier 1 banks... [reducing]

costs by 20-30% [via cloud deployments compared to on prem]... which [for one client] equated to \$12m+ savings over five years<sup>59</sup>. The other key attraction of cloud is the speed of deployment which can be in a few days or weeks compared to four to 12 months via on premises.

The main concern remains security and handing over sensitive data to a third party, with all the risks entailed.

### Deployment model considerations for Cloud and On Premises

|                | <br><b>Public Cloud</b>   | <br><b>Private Cloud</b> | <br><b>On Premises</b> |
|----------------|--|--|---|
| Implementation | Up to 4x faster than on premises; key challenge is regulatory approvals  |  | Slow due to initial build and set up of additional IT   |
| Owner          | Cloud service provider   | Single organisation with support from cloud service provider   | Single organisation has full autonomy over how the solution is managed on their servers                   |
| Security       | Medium security. Can be strengthened through use of permissions settings, penetration testing, data encryption, IP address whitelisting and more | Higher security  | Highest level of data security  |
| Management     | Managed externally by cloud provider   | Internal cloud team required for management  | Extensive management of internal infrastructure and tech required   |
| Scalability    | Very high scalability  |  | Not easily scalable   |
| Data recovery  | Extensive data recovery and archiving capabilities   |  | Weaker data recovery and business continuity processes  |
| Efficiency     | Potentially low, resources for running and managing the solution are shared with other firms   | Higher efficiency as private server guarantees bandwidth availability                                      | Vendor access to the solution is not direct meaning updates and customisation may take more time          |
| Cost           | Low cost as no requirement for internal IT infrastructure. Predictable monthly/annual ongoing costs which include maintenance                    | Slightly higher cost for private cloud space and dedicated IT support for operations                       | High initial investment required for IT and infrastructure support. Ongoing maintenance costs also high   |

Source: Capco

## Chapter 2

# SOLUTION SELECTION CRITERIA AND DEPENDENCIES

Before discussing the key differentiators across vendor solutions, it is worth pausing to consider the question of buying (via a vendor) versus building in-house. Almost all major financial institutions, with one or two exceptions, utilise external vendors for the majority of their surveillance needs, not least as it tends to be more cost-effective and dependable.

### Buy vs build – key considerations

|      | Buy with a vendor   | Build in-house  |
|------|---|---|
| Pros | <ul style="list-style-type: none"><li>• Lower cost</li><li>• Quicker implementation time</li><li>• Enables time and resources to be focussed on business development activities</li><li>• Potential to buy whole suite of financial crime solutions to have integrated offering</li></ul> | <ul style="list-style-type: none"><li>• Greater flexibility</li><li>• More control</li></ul>  |
| Cons | <ul style="list-style-type: none"><li>• Less bespoke</li><li>• Dependent on vendor</li></ul>  | <ul style="list-style-type: none"><li>• High costs</li><li>• More risky</li><li>• Cannot easily leverage shared industry learnings</li><li>• Distracts focus from revenue focussed activities</li></ul> |

### Vendor landscape

There are up to 30 leading trade and communications surveillance providers each with their own unique background, target segments, and functional/technical attributes – for example:

**Longstanding providers:** The longest running and best known incumbents include Nasdaq SMARTS (established in 1994) and NICE Actimize (established in 1999), which between them hold circa 50% of the market; the other firm with a particularly long pedigree is B-Next (founded in 1989). A cluster of newer entrants have entered the market particularly since the early to mid-2010s, including Trading Hub, Scila, Eventus, SteelEye, Trillium and Behavox, who have won market share with their generally lower price points.

**Buy side specific solutions:** ACA Group focuses on the buy side; NICE Actimize also offers a buy side specific solution. Nasdaq SMARTS previously offered a buy-side solution however, now like many others, it adapts its core solution as appropriate to buy-side clients (e.g. switching off non-required alert scenarios and functionalities).

**Specific to or specialising in certain asset classes:**

Whilst most providers cover all asset classes, Solidus solely focusses on crypto and DeFi (Decentralised Finance); and Trading Technologies is best known for its futures coverage (though it has recently expanded to cover other core asset classes). Eventus' solution, whilst in usage across the financial services landscape, is particularly in demand by centralised crypto exchanges; and Nasdaq SMARTS is also making a large

play in the crypto space and currently services circa 10 crypto exchanges.

**Holistic surveillance providers:** Some solutions offer both trade and comms surveillance themselves (i.e. without relying on any partners) – these include NICE Actimize, SteelEye and Kaizen.

**Generic solutions which can be tailored to surveillance:** Software AG's complex rules-based solution can be tailored to use case and client need, with one use case being surveillance.













**Provision of additional compliance or business services:** Some firms specialise solely in trade or communication surveillance; others such as NICE Actimize offer a host of AML and compliance related services. OneTick offers market data services, transaction cost analysis. FIS offers AML and personal account dealing services. Nasdaq SMARTS, post its Verafin acquisition in 2021, also offers AML and fraud solutions.

**Other:** Some firms differentiate themselves through their ex-regulator expertise such as ACA; others via their links to academic institutions and deep coding/development knowledge such as Scila. Some firms, such as ACA and Broadridge, have associated consulting divisions which can provide tailored advice on alert calibration.

Shortlisting and selecting the vendor that best fits your requirements can be a time consuming, challenging and high stakes exercise – especially, on the basis of short demos and a selection of marketing materials – when the cost and implications of arriving at the wrong decision can run into the tens of millions, and take years to unpick.

Over the following pages we outline 12 key criteria for evaluating surveillance solutions. The evaluation of a solution and its benefits must also consider dependencies with your organisation's technology and data architecture as well as your compliance operating model.

### Key solution selection criteria

| Target client and alerting   | Holistic surveillance   | Pricing   | Other   |
|--|---|---|---|
|  Target client                  |  Data                        |  Pricing |  Case management     |
|  Alerting and alert calibration |  Holistic surveillance       |   |  Additional services |
|  Asset class coverage           |  Communications surveillance |   |   |
|  Machine learning and analytics |  Market data provision       |   |   |
|  |  Cloud technology            |   |   |

Source: Capco



## 2.1 TARGET CLIENT AND ALERTING

### Target client

Depending on whether you are a sell side or buy side firm; or a market operator (for example exchange or regulator) you will have different solution needs:

#### Buy side firms

- Alert scenarios are different – the top fear of buy side compliance officer is insider trading, which if severe enough, could put a firm out of business; many sell-side relevant scenarios such as wash trading are less important, except prior to month- and quarter-end (re)valuation periods
- Asset class coverage tends to focus on equities and fixed income
- Data requirements are different – for example positional data is key showing overall holdings in each fund or security
- Certain functionality such as market visualisation replays are not needed, and the same level of optionality with dashboards is not required especially given the typically smaller number of in-scope employees.

#### Sell side firms

- A wider range of alert scenarios is required, typically 20+
- Asset class and product coverage is broader than for buy side, for example to cover FX and derivatives
- Communications surveillance is required for both sell side and buy side to help with unmasking “intent” and fulfilling regulatory requirements
- Data scalability is key especially for the high frequency algorithmic trading firms and large Tier 1 firms; in addition, for HFTs, real time surveillance is important to ensure algorithms are not causing real time disruption to the market.

#### Market operators (exchanges and regulators)

- Alert scenarios will tend to be broad to cover all key scenarios
- Asset class coverage for exchanges will naturally focus on equities and exchange traded derivatives; and for regulators will cover all asset classes
- Communications surveillance is not required
- Data scalability is key for exchanges – in particular the ability to process millions of messages per second
- Real time (rather than T+1) monitoring to enable systemic issues to be promptly resolved.

## Alerting, calibration and minimising false positives

Vendors tend to have upwards of 100 'out of the box' alert scenarios that are monitoring for different types of market abuse though these are typically different flavours of a core set of around 20 market abuse scenarios, including: insider trading, layering/spoofing, wash trades, marking the close etc. Cross-product and cross-market alerting always involves one of the above core market abuse types.

FIs will select, often with assistance of the vendor, the subset of scenarios most relevant to their business, as identified through their risk assessments.

### Calibration

Alert scenario parameter thresholds (e.g. look back and reference time periods) need to be calibrated during the initial implementation phase and thereafter reviewed on a regular basis to ensure they remain effective – i.e. that the models are not under- or over-calibrated. Relying on OOTB (Out of the Box) settings is a seldom used practice and is often flagged by regulators including the FCA – e.g. Market Watch 48 (June 2015), 56 (September 2018) and 69 (May 2022) – as not being in line with MAR requirements.

Key calibration related considerations include:

**Vendor-led or self-calibrated:** Some vendor solutions exclusively limit calibration to being performed by the vendor; others enable self-calibration whether through updating programming code (e.g. Python<sup>®</sup>) or through adjusting drop down fields indicating the thresholds for an alert's five to 10+ parameters. Some vendors such as ACA Compliance have multiple ex-regulators on their staff who can advise clients particularly during the initial calibration period.

**Backtesting:** As a good practice most vendors offer integrated UAT environments to backtest new rules/parameter calibrations and see how many alerts are generated before implementing the new rules in a live environment. Any changes can be tested on either historical or live data.

**Reporting:** Weekly and monthly MI reports can be reviewed to flag any issues with alert calibrations – the FCA in Market Watch 47 (March 2015) noted MI could identify "deviations

in alert frequencies that may indicate alerts are no longer appropriately calibrated." Machine learning reports can also suggest finetuning of parameter thresholds.

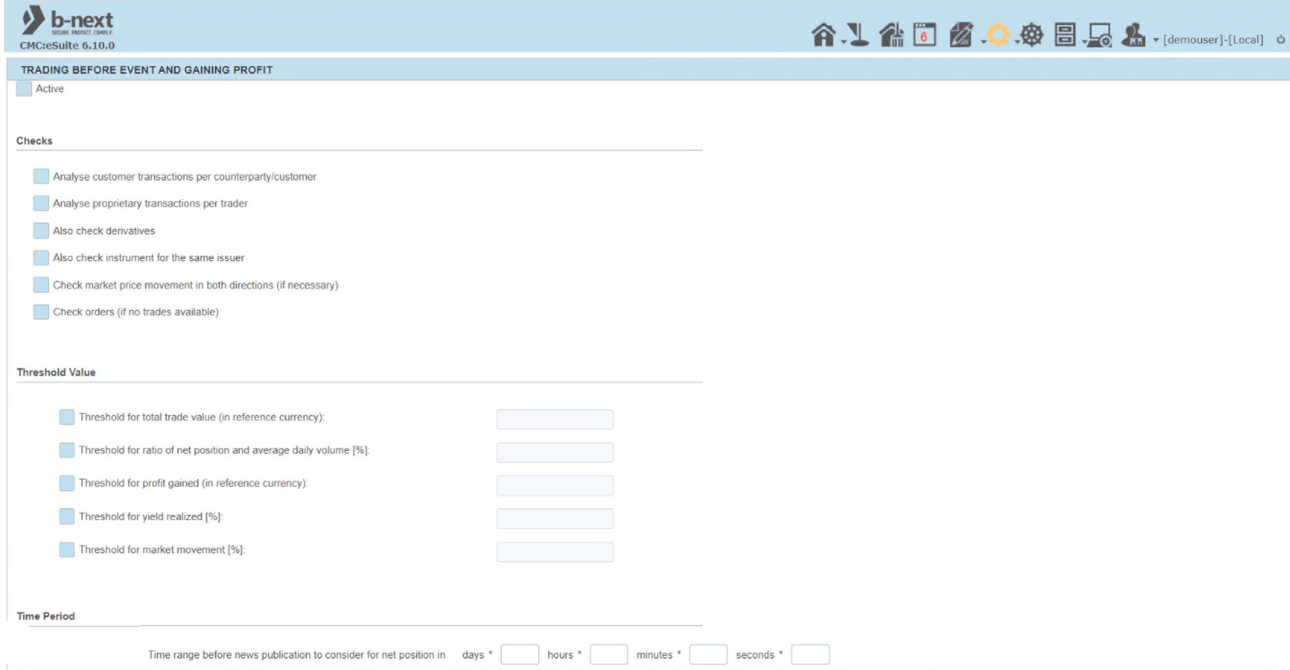
**STOR levels:** Another angle considered by clients in the context of alert calibration, particularly when running Proofs of Concept with vendors, is the quantity and quality of STORs (Suspicious Transaction and Order Reports) identified; as this is a key metric regulators utilise when benchmarking firms.

### Additional approaches to minimise false positives

**Alert triaging:** Many vendors build metrics around alerting that effectively 'triage' the alerts by importance ensuring those most likely to constitute market abuse are reviewed as a priority. This can take the form of:

- **Scoring** – alerts can be scored as high/medium/low, or 0-10 based on the extent to which parameters and thresholds have been breached. And with many vendors, parameters are weighted to ensure the highest risk alerts are prioritised
- **Market value of the potential market abuse** – Trading Hub's approach is to highlight the potential size value of the market abuse incident so for example any incident with a potential impact of less than \$500 can be deprioritised
- **Machine learning** – covered in more detail in the previous section and page 20, machine learning and AI approaches can predict based on past alert outcomes which alerts are most likely to be true positives and either assign a score or high/medium/rating to help compliance analysts focus their efforts accordingly.

**Dynamic benchmarking:** By considering a trader's positional data, and the average daily market or customer price volatility, this can help avoid spikes in alerts during periods of market volatility (e.g. if a stock moves by 10% and a trader trades ahead of that move, how much of that move is related to the broader market and therefore not an indication of insider trading).



b-next: Configuration window for Trading Before Event and Gaining Profit alert. Client can input thresholds for abuse detection

### Asset class

The majority of vendors cover all key asset classes (e.g. equities, fixed income, FX, derivatives), with some vendors’ coverage extending to commodities, crypto and energy. That being said, some vendors specialise in certain asset classes; and a small number of vendors, as mentioned earlier, focus exclusively on a single asset class/product.

The alert scenarios tend to be generally the same across each asset class, though with tailored parameter and threshold calibrations to account for the asset class’s specific features, trade lifecycles and data accessibility. Two particularly challenging asset classes to surveil are fixed income and crypto.

Fixed income, whilst it can be exchange traded via MTFs

(multi-lateral trading facility) is largely OTC traded and hence presents not insignificant challenges – especially outside the US – with obtaining comprehensive pricing data upon which to run monitoring. IHS Markit (recently acquired by S&P Global) is considered the leading provider of OTC fixed income data.

Crypto monitoring, whilst less of a pressing priority since the crypto scandals of 2022, is a service vendors increasingly offer, and firms are interested in exploring. Key differentiating features include real time monitoring (given crypto’s 24/7 nature), access to comprehensive crypto trading data, ability to account for different product types (on and off chain; smart contracts; spot and futures etc.), and ability to support the latest regulations including MiCA and the Travel Rule.

## Machine learning and analytics

In the trends section, we touched on the increasing openness of both regulators and financial institutions to utilising supervised and unsupervised learning – in particular, leveraging supervised learning to prioritise alerts and feed into the parameter recalibration processes. Machine learning uptake has been most prevalent amongst larger FIs. It is little surprise therefore that vendors, whilst previously somewhat ML averse, have in the last one to two years increasingly incorporated machine learning functionality into their solution offerings.

In the comms surveillance section below, we cover the usage of other machine learning use cases such as NLP. Here it suffices

to discuss one additional key analytical approach, namely behavioural profiles. Such profiles can facilitate moving from an event-driven/alert-based model to a trader-centric view of risk. Based on a variety of sources including past trade and communications surveillance alerts, P&L, HR and other internal data, a risk score is assigned to traders. This can be used to support the triaging of alerts with the review of alerts of higher-risk traders prioritised. The main vendor championing this approach is NICE Actimize – with its SURVEIL-X solution; and KX. Regulators are yet to opine in detail on this emerging trend.

## 2.2 HOLISTIC SURVEILLANCE

### Data

For a surveillance solution to operate alerts, both a firm's transaction/order data and market data (including market news) needs to be ingested and analysed. There are number of key data considerations including data ingestion and harmonisation approaches, scalability and recovery.

**Data ingestion:** There are two main approaches for ingesting a firm's transaction/order data: either batch updates at end of day via drop-copy files or direct feeds via API. Larger FIs as well as exchanges tend to use APIs; whereas smaller FIs and buy side firms are more open to drop-copy file approaches.

**Data harmonisation:** This is one of the most complex and time-consuming aspects of a solution onboarding; and fundamental to effective operation of your chosen system. The key information requiring normalisation consists of around 40-50 fields including trader IDs (across various platforms), order and execution time stamps, customer names, and instrument codes. This is a significant reduction on how solutions previously operated with up to 300-400 fields previously required.

Data can either be normalised by the FI itself to align with a fixed vendor format; alternatively, many vendors offer to

normalise the data to either align with a fixed format, or with a flexible data schema. Oftentimes larger FIs or those who have a strong data foundation will opt to normalise the data themselves, with smaller FIs opting to allow the vendor to normalise the data.

**Data scalability:** It is vital to consider whether a vendor can handle and manage the volume of data required by your institution; many of the newer, smaller vendors do not yet have the infrastructure to support large Tier 1 clients and exchanges. This may be in terms of their IT and server capabilities not being able to handle the volume of data (large exchanges can be required to handle billions of messages per day – OneTick for example can handle 500 billion+ messages per day), or not having the internal resources to support implementation.

**Data recovery:** Given the increasing regulator focus on operational resilience, it is important to consider a vendor's data recovery capabilities. Different approaches have been adopted by vendors including access to multiple servers, tracking of server crashes and live data replication environments (for example in an alternative region). The data recovery functionalities offered by cloud deployments are a particularly attractive feature for a growing number of FIs.

## Holistic surveillance

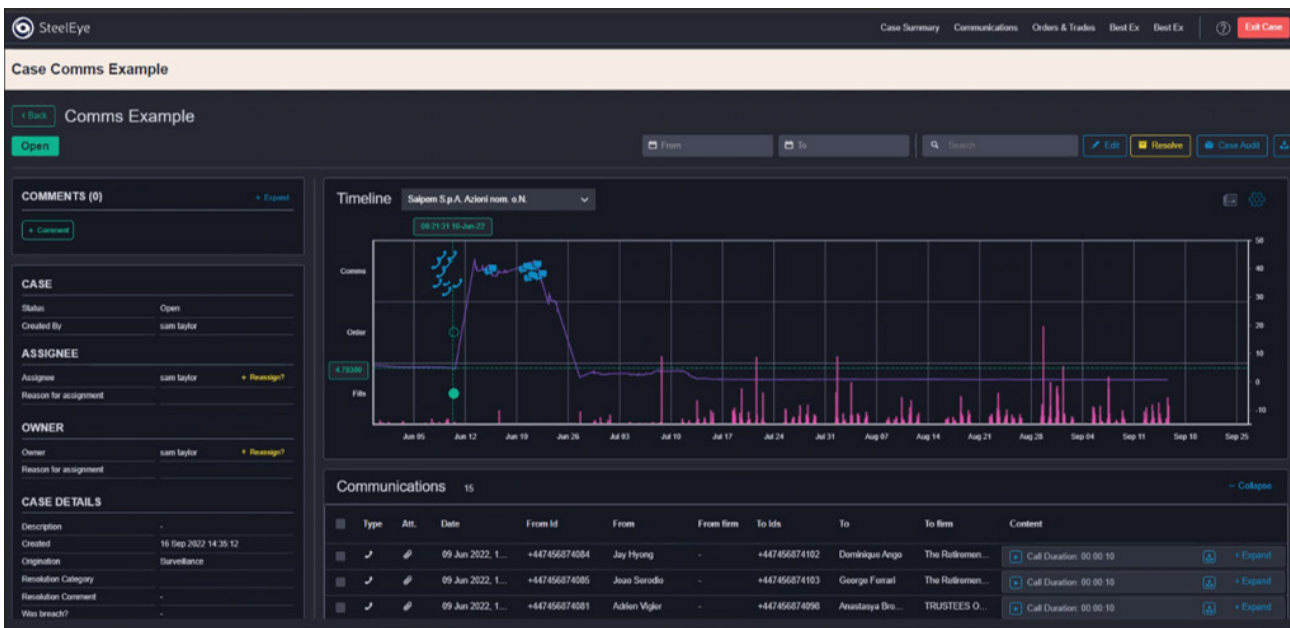
As touched on in the trends section, holistic surveillance is increasingly sought by FIs – given the significant benefits offered. These include a reduction in false positives and improved risk detection by breaking down the ‘Chinese Walls’ between different solutions, reduced time manually stitching together disparate sources to assess an alert, reduced costs in the long-term, and the ability to effectively meet MiFID II and Dodd Frank trade reconstruction requirements.

Vendors' holistic surveillance offerings broadly span three categories:

- Holistic trade and communications surveillance via a single provider
- Holistic trade and communications surveillance via an integrated case management system (i.e. still utilising multiple separate vendor solutions)
- Holistic financial crime case management system (integrating surveillance, AML, sanctions and other financial crime data).

A limited number of vendors offer a single provider solution for trade and communications surveillance – these include SteelEye and NICE Actimize; NICE Actimize additionally offers more comprehensive holistic financial crime case management. An increasing number of vendors are setting up partnerships to effectively ingest alerts into an integrated case management system – this includes FIS and Shield. Whilst this approach allows you to benefit from your preferred solutions for each surveillance use case it does mean there remain two user interfaces and two sets of data.

Holistic approaches tend to be of most benefit right now to smaller and mid-sized banks, as well as asset managers. This is because of the significant data challenges (data normalisation, linking of comms data to trader/trade, combining data sources via a data lake or data abstraction layers), and complexities of ripping out and replacing the multiple vendor solutions implemented across most FIs.



SteelEye alert view: communications and trades overlaid and correlated in one alert

## Communications surveillance

Functioning similarly to trade surveillance, comms surveillance solutions capture and ingest communications data from multiple channels, with the communications then surveyed by alerting rules. The communications data can also be archived. Vendor solutions cover all or some of these aspects.

**Capture (and archiving):** Differentiators between vendors include the number of channels covered (some solutions state they can capture up to 100 or even 150+ channels – including email, telephone, Whatsapp/WeChat/Signal, Bloomberg/Reuters, Teams/Zoom etc.); how frequently data is ingested (daily or weekly); usage of multiple point solutions vs open APIs; and finally whether utilising relational or non-relational databases – non-relational databases (e.g. NoSQL and Hadoop) are becoming an increasingly popular means of capturing unstructured data.

Archived data also needs to align with regulatory recording requirements – for example, the EU requirements for data retention for up to seven years, ability to retrieve within 72 hours and be captured in an immutable format (“write once, read many”).

**Monitoring:** Depending on regulatory requirements, firms tend to follow different approaches: some pro-actively monitor all (or a sample of) communications, others only review communications during active investigations.

Given the trend towards more comprehensive communications surveillance it is key to ensure false positives are minimised (to avoid the need for hiring hundreds of extra compliance staff). A number of approaches are being utilised:

- **Customisable lexicon sets** – whilst all communications surveillance providers will have large pre-defined lexicon sets, many also allow the user to create their own lexicon library. This can include terms, client names, abbreviations, and slang that may be specific to their organisation. For example, for an organisation trading FX or with Canadian counterparties the term ‘Loony’ may often be used as slang

for the Canadian Dollar. Kaizen allow clients to send them a list of personalised lexicons via .csv file which are then integrated into the system.

- **Smart lexicons** – rather than simply operating with the crude lexicon approach of flagging alerts based on key words or key phrases; smart lexicons utilise sophisticated scoring models and other matching models (including Boolean, proximity etc.) are utilised to increase the likelihood of a match being found – for example the message “let’s discuss this on WhatsApp in accordance with the rules”, the WhatsApp reference would be offset by the phrase “in accordance with the rules”, so would register a lower scored alert than “let’s discuss this offline on WhatsApp”.
- **NLP (Natural Language Processing)** – NLP takes this approach a step further by considering the context of a whole sentence. An enormous library of sentences associated with market abuse is constructed; the NLP model, leveraging logistical correlation and regression methods, flags whenever there is a close match. And the closeness of the match can itself be tweaked so that, for example, it only flags where there is a 90% match. In addition, the accuracy of the models is continuously improving as most utilise a supervised learning approach. Behavox, a pure-play comms monitoring provider, claim NLP can increase the true positive rate from by as much as 10-20 times. Many FIs are adopting a blended approach with lexicon based models serving as a first line, and NLP solutions acting as an additional layer to prioritise high-risk alerts.
- **Non-business related communications** – a combination of lexicon approaches and machine learning can be used to identify newsletters or non-business emails and discount these from raising alerts, if for example it states in the email “join us on WhatsApp”.

- **Employee conduct scores** – as with trade surveillance and usage of behavioural profiles to identify individuals of highest risk, the same approach can be followed in comms surveillance; those individuals who have been separately highlighted as high risk, or who have been subject of multiple alerts can be prioritised for review. NICE Actimize is currently in beta testing with a select group of Tier 1 banks building out and testing this capability.
- **Entity matching and holistic surveillance** – to tie communications to a trade so alerts can be overlaid on a single timeline, various data points are considered (including the trader email address, phone number, account/platform IDs, having a list of acronyms for banks, instruments etc.). Some vendors such as VoxSmart utilise complex AI algorithms to assess the probability of the communication being linked to a given trade.

Other key functional use cases offered by vendors include sentiment analysis, metadata analysis (in particular, relationship mapping), and data breach avoidance.

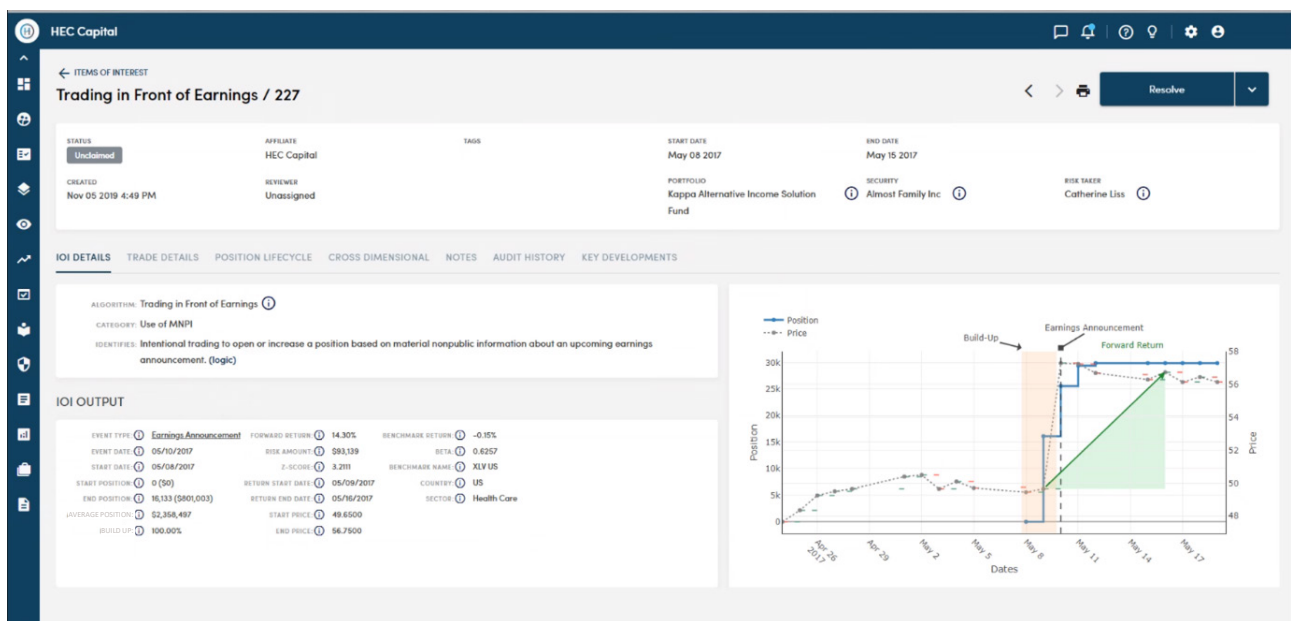
Firms should also consider their approach to voice comms (otherwise known as acomms). Key aspects include:

- **Language transcription** – transcription capabilities are vital as the voice data needs to be transcribed and sometimes translated prior to analysis using lexicons and NLP technologies. In addition to the quality of a vendor's transcription technology, key vendor differentiators include the number of languages covered (some vendors can transcribe up to a dozen languages), and the ability to manage language switching.
- **Recording quality** – particularly important is the recording quality post archiving and compression.
- **Recording checks** – instead of relying on manual recording checks, some vendors (such as NICE Actimize's NTR-X solution) offer automated recording check capabilities.

## Market data and news provision

Market data is, along with a firm's transaction/order data, a key component in the surveillance solution's analysis of trades and generation of alerts. Firms can either choose to utilise market data provided by vendors (typically Bloomberg, Refinitiv or S&P Global), or the vendor can integrate with your existing market data sources. The benefit of the former approach, apart from potentially reduced data costs, is that the market data is already harmonised to work with the vendor solution. Clients opting for Nasdaq SMARTS's solution benefit from ready access to exchange data from its 10 global exchanges.

News data is also important and plays an important role in detecting certain market abuse behaviours, in particular insider trading. With more holistic surveillance solutions, the relevant news is overlaid next to the alert. Again, there is the option to either utilise the vendors' news data provider or for the vendor to integrate your own existing data provider. In addition to the typical news providers (such as Dow Jones, Bloomberg, Reuters), some vendors utilise newsfeed consolidators. Trillium, for example, uses NewsWare which leverages over 100 sources including Dow Jones, Bloomberg and others.



ACA Compliance: Trading in Front of Earnings example

## Cloud

As discussed in the trends section, many financial institutions are showing increasing preference for cloud-based deployments.

Vendors' cloud based solutions should be considered based on criteria including their choice of cloud provider (e.g. AWS, Microsoft Azure, Google Cloud) and its alignment with your overall technology architecture, the availability of both public (multi-tenant) and private (single-tenant) cloud functionality, the

vendor's data security protocols (including certifications such as ISO27001, SOC 2 and NIST), their ability to navigate regulators' data hosting requirements, and experience with data migrations.

Newer vendors generally offer cloud only deployment, and for smaller firms, most vendors will only offer cloud deployment. Larger banks and high frequency trading firms still tend to prefer on premises installations (or hybrid approaches, utilising on premises data storage for the most sensitive data).



## 2.3 PRICING

The cost of engaging with a vendor consists of two main charges: an up-front implementation cost and a recurring maintenance fee (some vendors split this maintenance fee into a license fee for usage of the solution, and a support fee covering any upgrades, and IT/vendor resource support).

Each vendor has its own pricing structure typically accounting for the following components:

- Number of alert scenarios
- Number of asset classes
- Trading volumes
- Number of exchanges & locations
- Number of monitored employees
- Deployment model – cloud vs on premises
- Calibration – extent of alert parameter customisation support
- Real time vs T+1 alerting
- Data normalisation – whether undertaken by FI or vendor
- Ongoing vendor support levels
- Provision of complementary services e.g. transaction reporting, best execution

With communications surveillance, there are other relevant criteria, including the number of languages and communication channels covered; and whether the solution scope encompasses recording, archiving and monitoring; or a sub-set of these.

Three points are worth noting. First, naturally the more comprehensive your surveillance package the more you can benefit from reduced pricing (for example if utilising a vendor's comms and AML offerings in addition to trade surveillance; or if expanding coverage to include additional locations).

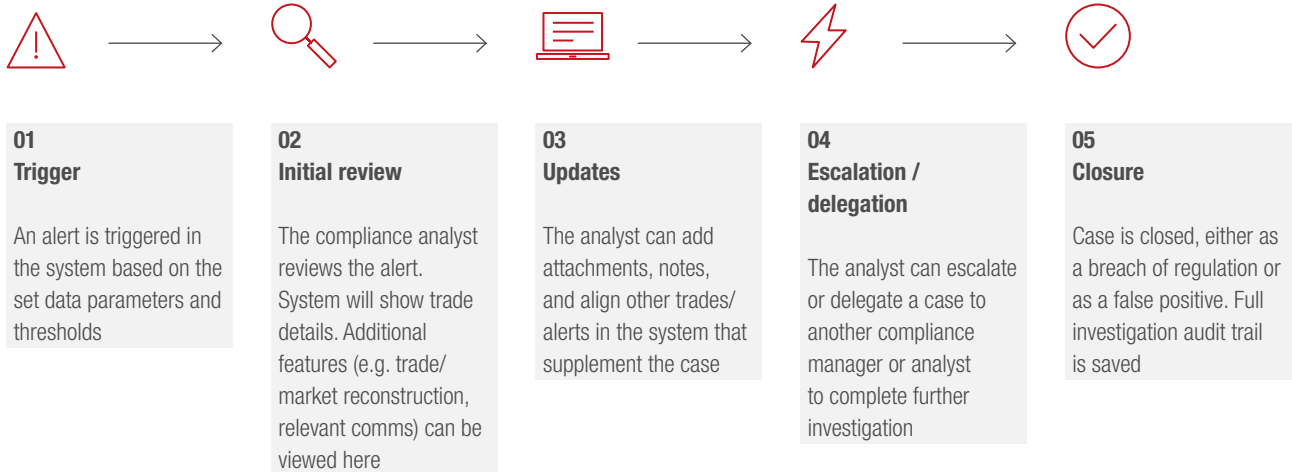
Second, it is important to consider TCO (Total Cost of Ownership). Some vendors have low entry price points, but require a significant number of add-ons to deliver an effective solution. You may also benefit from a vendor's broader capabilities. For example, Kx Surveillance has KDB+ technology underlying their data ingest. KDB+ can process billions of rows of data a day, and they have reported previous cases where an existing solution was replaced with Kx and the required drive space decreased by 90%.

Finally, the old dictum "buy cheap, buy twice" should always be borne in mind. Whilst cost is a key consideration, what is vital is getting good value for money – and this will mean different things to different clients.

## 2.4 OTHER FACTORS

### Case management

Most solutions offer a standard case management workflow.



Source: Capco

Other additional features useful to consider, include:

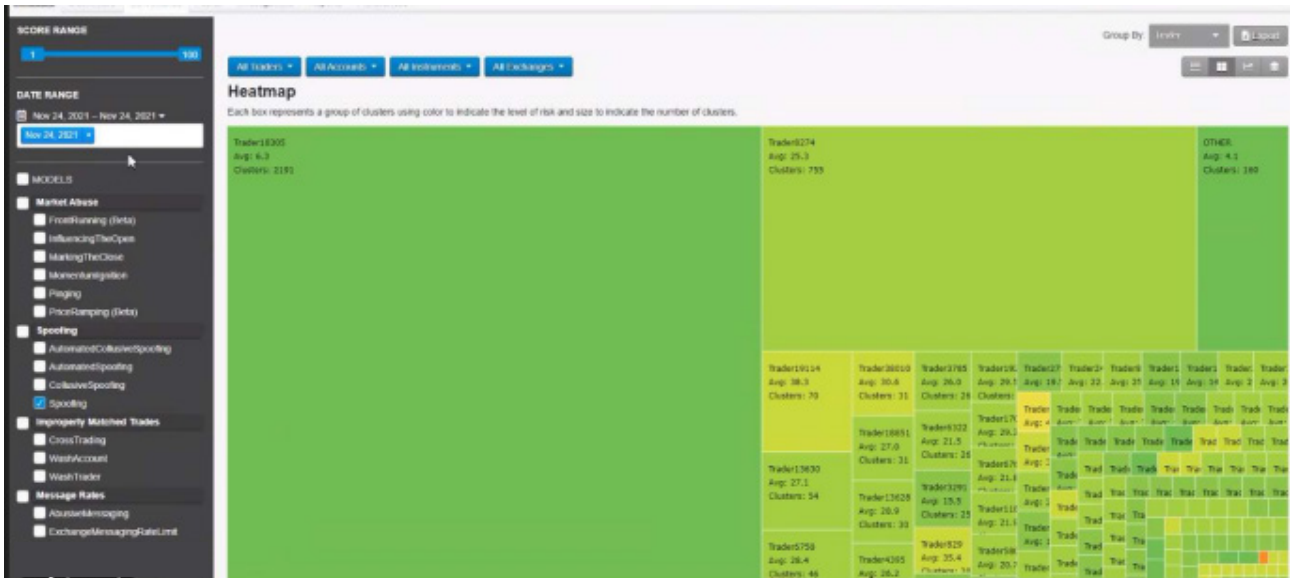
**User Interface:** Arguably, newer providers often have more modern user interfaces enabling a more intuitive approach to case management. That being said, amongst longstanding providers Nasdaq SMARTS, for example, recently launched a revamped UI which includes advanced dashboard filtering, market replay and alert recalibration visualisation functionalities. Below are shown two example UIs.

**Dashboarding and reporting:** Most vendors offer integrated BI dashboards, as well as OOTB and customisable reports. Dashboards and reports serve multiple purposes – providing a snapshot of alert volumes and types across the business, identifying alert scenarios which are mis-calibrated and need fine-tuning, and enabling filtering to zero-in on particular regions, desks, or traders.

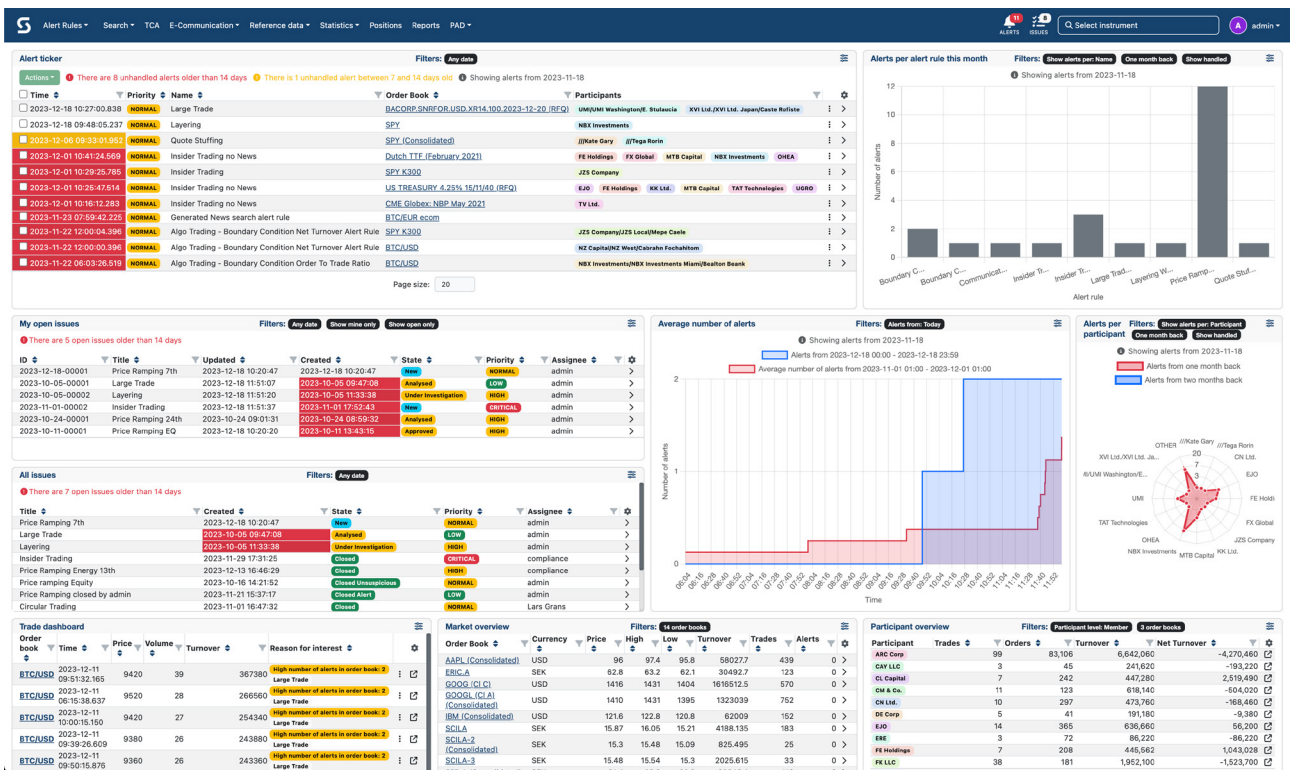
**Market Replay:** The market replay capability effectively puts the compliance analyst in the shoes of the trader who triggered

the alert. The trader's activity is overlaid with a full view of all trades, both bid and ask – including the full market depth order book data (also known as level 2 order book). Undoubtedly, this functionality gives context to unusual behaviour and empowers the compliance analyst to make a more informed decision as to whether an alert is a true case of market abuse – this is particularly helpful for uncovering instances of layering and spoofing.

**User permissioning:** Large financial institutions typically have a siloed internal structure. User permission capabilities implement controls around what certain groups can access, and what can be shared between groups. This ensures that the wrong information is not inadvertently shared (e.g. between public and private side, different jurisdictions, or first and second line teams) causing a regulatory breach or conflict of interest. Additionally, many solutions have the concept of a 'participant hierarchy' – for example, a manager may have the ability to bulk close alerts or calibrate parameters on existing alerts, whilst a junior analyst would not.



Trading Technologies case management dashboard: heat map view



Scila case management dashboard

## Other use cases for surveillance tools

Many surveillance vendors also offer complementary solutions – these, generally speaking, fall into three or four categories:

- Financial crime - AML, personal account dealing
- Other regulatory commitments - best execution, trade & transaction reporting, trade reconstruction
- Data insights - transaction cost analysis, sales and performance tracking
- Other - conduct and behaviour monitoring, Consumer Duty monitoring, market data services.

## Closing thoughts

As we have seen, market and regulatory drivers are reshaping firms' approaches to surveillance, with key trends including cloud adoption, AI and machine learning, and a move to holistic surveillance – the ambition being to reduce costs, minimise false positives and better identify actual risks.

Firms should assess vendor solutions based on these factors as well as others including vendors' asset class coverage, data scalability, data normalisation approach, and, of course, price point. Less tangible factors such as the experience, capability and responsiveness of a vendor's product team need to also be borne in mind.

Once a shortlist of vendors has been identified – in collaboration with Compliance, IT and the Business – it is important you run Proofs of Concept so each option can be compared, including against any incumbent supplier solution. Implementing a new or replacing an existing solution can be a costly and time-consuming exercise; it is therefore vital you undertake thorough

due diligence up-front to avoid mistakes which can take years to untangle. Capco can help in drawing up budget and implementation plans taking into account all dependencies and workstreams required to achieve a successful implementation.

It should also be remembered that any tool or system is only as good as the overall framework within which it is operating. Even the best surveillance system cannot make up for any major deficiencies in governance model, data quality, resourcing approach, training and culture – to name just a few factors.

**If you found this report useful and would like to discuss how Capco can support you in shortlisting, selecting and implementing a surveillance solution well-suited to your needs; or would be interested in receiving the addendum with summaries of the 20 vendors we reviewed, please get in touch.**

## REFERENCES

1. Alert and STOR volumes, as well as average bank surveillance spend is based on Capco market experience
2. The most recent comprehensive vendor landscape surveys include “Shortlisting Trade Surveillance Solutions” by Opimas (2018) and “Capital Markets Surveillance Vendor Landscape” by Celent (2018)
3. <https://www.steel-eye.com/news/steeeyes-surveillance-round-up-key-takeaways-from-xlod-2022>
4. SEC operates three supervisory technology tools: a) National Exam Analytics Tool (NEAT) – reviews investment advisor and broker dealer data prior to exams; b) High Frequency Analytics Lab (HAL) – detects high frequency trading issues; c) ATLAS – identifies insider trading before a major equity event and other insider trading examples
5. NICE Actimize paper, “4 Reasons to Move Trade Surveillance to the Cloud”, 2021
6. OneTick has specifically chosen Python as its programming language given its versatility and ease of use

## AUTHORS

Jonathan Lappage  
Bea Simmons  
Dan Young

## ADDITIONAL CONTRIBUTORS

Charit Arora  
Tom Oliver

## CONTACTS

**Jamília Parry**  
Partner, Financial Crime,  
Risk and Compliance  
[jamilia.parry@capco.com](mailto:jamilia.parry@capco.com)

**Emily Turner**  
Partner, Capital Markets  
[emily.turner@capco.com](mailto:emily.turner@capco.com)

**Jonathan Lappage**  
Principal Consultant  
[jonathan.lappage@capco.com](mailto:jonathan.lappage@capco.com)

---

## ABOUT CAPCO

Capco, a Wipro company, is a global technology and management consultancy focused in the financial services industry. Capco operates at the intersection of business and technology by combining innovative thinking with unrivalled industry knowledge to fast-track digital initiatives for banking and payments, capital markets, wealth and asset management, insurance, and the energy sector. Capco's cutting-edge ingenuity is brought to life through its award-winning Be Yourself At Work culture and diverse talent.

To learn more, visit [www.capco.com](http://www.capco.com) or follow us on Facebook, YouTube, LinkedIn and Instagram.

## WORLDWIDE OFFICES

### APAC

Bangalore – Electronic City  
Bangalore – Sarjapur Road  
Bangkok  
Chennai  
Gurgaon  
Hong Kong  
Hyderabad  
Kuala Lumpur  
Mumbai  
Pune  
Singapore

### MIDDLE EAST

Dubai

### EUROPE

Berlin  
Bratislava  
Brussels  
Dusseldorf  
Edinburgh  
Frankfurt  
Geneva  
London  
Milan  
Munich  
Paris  
Vienna  
Warsaw  
Zurich

### NORTH AMERICA

Charlotte  
Chicago  
Dallas  
Hartford  
Houston  
New York  
Orlando  
Toronto

### SOUTH AMERICA

Alphaville  
São Paulo

[WWW.CAPCO.COM](http://WWW.CAPCO.COM)

