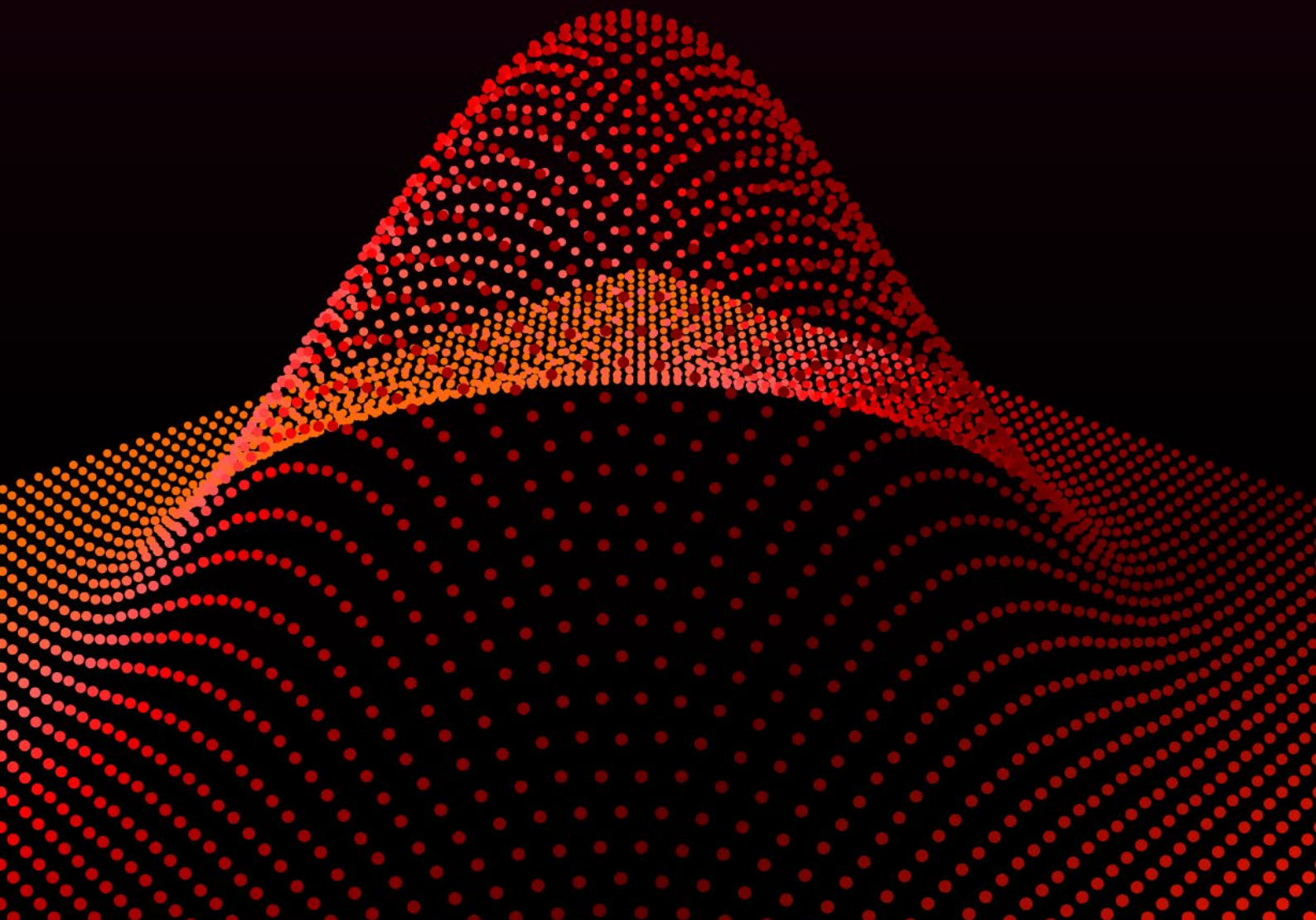
greyspark partners

Integrated Trader Surveillance

Identifying the Asymptote



Integrated Trader Surveillance

Identifying the Asymptote

Surveillance – specifically trader surveillance – in financial services institutions remains an area of focus for Compliance professionals in 2023. Generally comprising a combination of trade and communications (voice and eComms) monitoring, trader surveillance is driven primarily by regulatory demands. While there are specific obligations for trade surveillance set out in regulations such as EU's Market Abuse Regulation (MAR), the US's Dodd Frank Act (DFA) and Singapore's MAS-SGX best practice guide, the requirements for communications monitoring are less well-defined. Although MiFID II and DFA mandate the recording of communications and so-called 'trade reconstruction', the monitoring of communications for market abuse, while explicitly required in some jurisdictions, is not stipulated in detail, and this has resulted in a greater variation of process across the globe.

That said, there have been a few notable instances in the US recently where firms have been fined for failure to properly manage communications. In the UK, the Financial Conduct Authority (FCA) has reached out to compliance teams in several global financial firms in a fact-finding mission to ascertain each financial firm's approach to the use and surveillance of its employee communications channels. This suggests that financial firms are likely to increase their focus on communications monitoring in the coming months and years in response to closer regulatory scrutiny.[1]

The other major driver affecting change in the surveillance space is technological. The landscape has shifted significantly in the last few years with advancements in big data, cloud technologies and artificial intelligence. Machine learning and natural language processing (NLP), which GreySpark Partners has written about in detail in the past, have made it possible to automate both trade and communications surveillance in a way that simply would not have been possible before.[2]

Finally, the burden on surveillance teams continues to increase as business and working practices evolve. A recent example is the employee utilisation of more numerous communications channels in the post-Covid-19 world, which has enormously increased the complexity involved in effective communications monitoring.

The bottom line is that trader surveillance processes must keep pace with innovations in trading products and methods, and all this takes place in the context of the continual drive by financial firms to streamline and improve processes across their organisations. In this article, GreySpark discusses the drivers for financial firms to assess the effectiveness of their surveillance solutions and to explore the potential advantages of integrating specific aspects of their trade and communications surveillance.

The Myth of Holistic Surveillance

'Holistic' has been a buzzword on the lips of surveillance professionals for several years now – and, at a high level, each of them understands it to mean roughly the same thing – surveillance of trader activity using both trade and communications data to detect fraudulent activity, market abuse and misconduct. Many might even extend the definition to include use of supplementary data, such as, say, building entry logs or personal location data to enhance the results of the process.

However, it is harder to pin down exactly what 'holistic surveillance' means in detail – there is clearly a wide spectrum of expectation amongst regulators, compliance professionals, software vendors and other staff in financial institutions, ranging from simply having separate solutions in place for trade and communications surveillance, right through to the long-anticipated single solution across all assets and departments that queries all datasets seamlessly to alert on suspicious trader activity.

It is fairly clear that, whilst many are employing processes that would be placed towards the left-hand end of the spectrum in **Figure 1**, examples of implementations at the right-hand end remain vanishingly rare – perhaps even currently impossible with the technologies available on the market.

[1] The US Securities and Exchange Commission, 2022. *SEC Charges 16 Wall Street Firms with Widespread Recordkeeping Failures* [press release] 27 September 2022. Available at: <https://www.sec.gov/news/press-release/2022-174>. [Accessed 30 March 2023].
[2] Brotherston, J., 2022. *The Case for Artificial Intelligence in Communications Surveillance.* [online] Available at: <https://www.greyspark.com/the-case-for-artificial-intelligence-in-communications-surveillance-2/>.

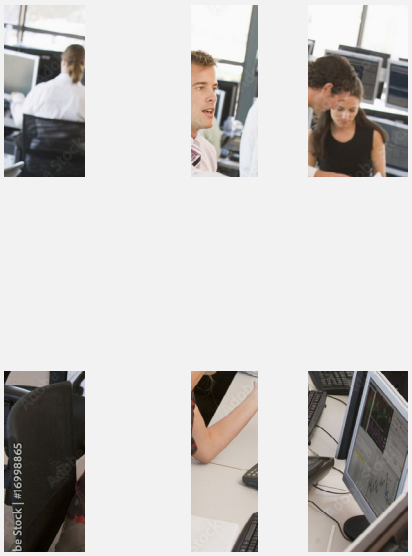
Figure 1: The Spectrum of Technology Solutions

Source: GreySpark analysis

Increasingly Sophisticated Surveillance Technology

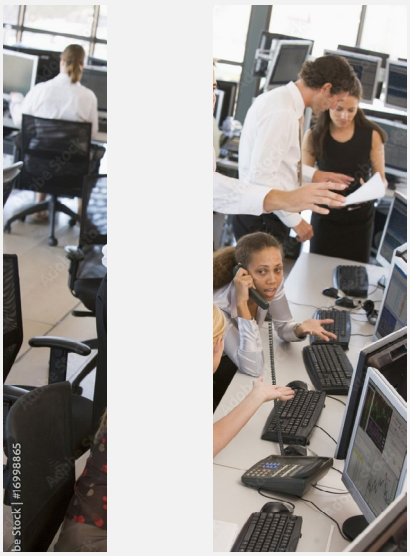
Little Integration if Any

Siloed surveillance and monitoring solutions - by department/asset class. Trade and communications managed in separate systems by separate teams.



Some Level of Integration

Integrated processes and software - as simple as a single team looking after the many surveillance platforms through to a network of individual software solutions that 'talk' to each other in order to achieve advanced analysis of the entire surveilled dataset.



Fully 'Holistic' Surveillance System

Fully 'holistic' surveillance system across the whole organisation - using all data indiscriminately - trade, communications, other - to perform all surveillance and monitoring compliance functions seamlessly with a high level of automation.

Some vendors offer a trader surveillance solution, with both trade and communications surveillance components and some vendors offer solutions that are able to integrate with other software platforms to provide the mutual client with two (or more) disparate solutions that can be viewed through a single user interface. Even they, it seems have limited capacity for seamless analysis across the entire dataset. It also appears that there are not yet many institutions who have built their own fully integrated surveillance solutions. Most still have separate software platforms – and sometimes separate teams – for trade and communications surveillance. There are also instances of separate solutions for individual departments or asset classes.

Despite the implication that 'full integration' of trade and communications surveillance capabilities in one platform is still not fully viable, it is still beneficial for institutions move their focus in that direction, towards what can be offered in the middle of the surveillance spectrum, rather than waiting for the 'perfect' solution to become available. Surveillance solutions that are integrated, but not yet fully holistic, move the financial firm's surveillance capabilities incrementally towards the right-hand side of the spectrum as the technology evolves.

Integrated Surveillance

There are a great many datasets that could or should be employed in surveillance analysis, most of which are already used in at least one of the 'standalone' surveillance platforms, some of which are shown in **Figure 2**. For example, news, communications, trade and market data could be combined to detect insider trading, a simple example of which is illustrated in **Figure 3**.

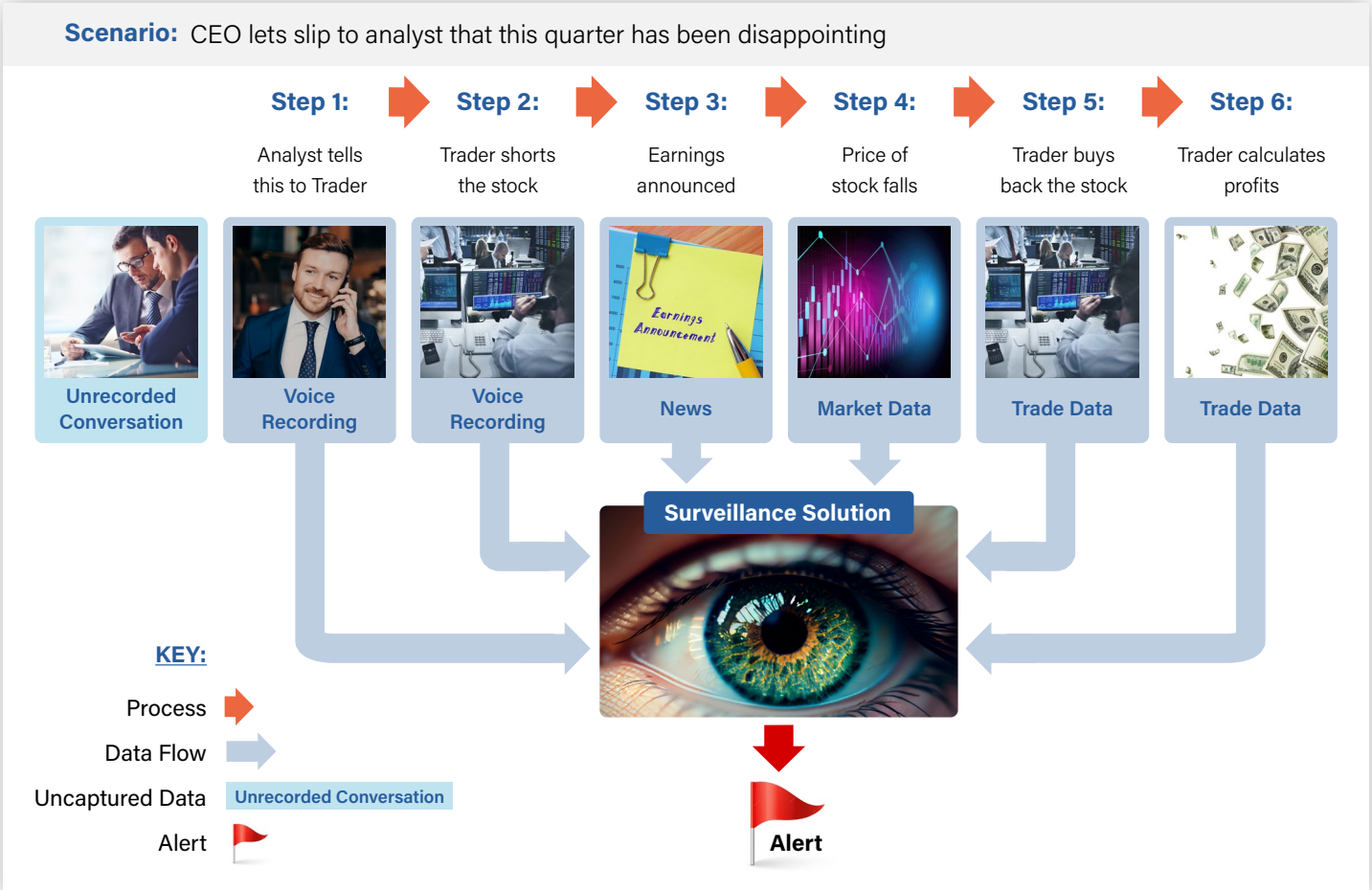
Being able to see a trader making large trades, after speaking with people outside their usual network, logging into unusual applications or accessing the building outside normal times, would not necessarily, in isolation, raise suspicion, but viewed together could identify a person trying to secretly cover losses for example.

Figure 2: Datasets That Might Fill in the Blind Spots of a Siloed Surveillance System

Source: GreySpark analysis

Figure 3: Data that Could Enhance Surveillance Efforts to Uncover Insider Trading

Source: GreySpark analysis



There is a wide spectrum of possibilities for what an integrated surveillance process – using several sources of data seamlessly in combination - could look like, including, but not limited to the examples shown in **Figure 4**.

As noted in the introduction, pressure from regulators is increasing, data is becoming more complex and surveillance technology is able to do a great deal more than it could even just a few years ago. As such, many incumbent systems and processes are beginning to feel creaky, old-fashioned and no longer fit for purpose. At the same time, the much-fêted fully holistic solution is unlikely to be an option in the immediate future, so investment in interim solutions will likely be required if breaches and fines are to be avoided. As such, investment in some kind of integrated solution or solutions would represent not only a step on the path towards fully holistic surveillance but would also be a useful goal in itself.

As well as being efficient, even the initial – seemingly minor - step of a single person or team being able to see all data and alerts in a single platform could help to **streamline processes** and begin the journey of bringing trade and communications surveillance and analysis together into one place. Even if it is only on a small scale to start with, the **increased capability** that arises from having the ability to utilise information from trade, communications and other datasets in combination to give context and improve outputs is valuable in itself, as well as being one step closer to a fully integrated solution. Finally, there are potential cost savings as a single platform is often cheaper than multiple platforms, as well as being simpler and more streamlined.

Figure 4: Examples of Integrated Surveillance Processes

Source: GreySpark analysis

1

Both trade and communications surveillance in a single platform

While the trade and communications surveillance are entirely separate in terms of analysis, a compliance analyst can now see both in a single UI or dashboard.

2

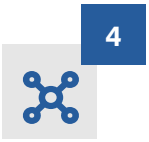
A single platform including separate solutions that can 'talk to' each other

As well as showing both sets of data, analysis and alerts in one place, searches, filters and further manual or automated analysis can be done within that dashboard. For example, the analyst could pull up all trade and communications alerts on a group of users and the solution would display visualisations or analyse patterns within that information.

3

Automated trade reconstruction

A sufficiently integrated platform would allow the automated reconstruction of trades as required by MiFID II or DFA. An analyst could specify a trade and the algorithm would automatically collate all communications and other data relating to the execution of that trade.



4

Stand-alone solutions that can ingest data from other platforms

This type of platform improves its own capabilities and alert generation incrementally by ingesting other data to enhance its alerting capabilities. For example, a communications surveillance platform could ingest specific alerts from a trade surveillance platform or data from the 'other' bucket. This data could then be analysed, manually or automatically, within the platform to give better context to alerts.

Different Strokes for Different Folks

Every organisation has different requirements for integrated surveillance and this is reflected in the many different platforms and processes implemented in the market. Firms looking to change their trader surveillance technology should be mindful of the following three key considerations:

1. **Business focus varies significantly from firm to firm**

   Some firms focus on a single asset class, client or counterparty, while others trade a huge variety of complex instruments involving many clients, counterparties and stakeholders. How much it is desirable or possible to integrate surveillance platforms and processes will vary accordingly, as will the business appetite to do so.

2. **Regulatory demands differ across different jurisdictions and different types of business**

   In many geographies, regulators are likely to focus attention on the big players in the market – or those with the most sensitive client base – and to offer more leniency to smaller parties initially, which in turn leads to different levels of surveillance and integration.

3. **The shape and size of an organisation will certainly lead to different requirements, priorities and resources**

   A larger organisation will have a far greater volume of data to store and analyse, which could infer more surveillance and integration possibilities, but will almost certainly also involve more complexity. A very small organisation, on the other hand, may not require much automation of communications surveillance at all and a simple manual approach may be sufficient. The degree to which departments are siloed will also have an impact. There may be less appetite for cross-departmental streamlining in a siloed organisation than in those firms with more assimilation of the different parts of their business.

In summary, the appropriate level and integration of surveillance systems and processes is likely to vary significantly between organisations.

Find Your Asymptote

Once again, surveillance is a hot topic for compliance professionals across financial services, and many are finding that their existing solutions are no longer fit for purpose in a world of increasingly complex business and organisational structures and with increasingly strict regulation and technologically savvy regulators.

While 'holistic surveillance' is still frequently discussed, it is clear that it may still be some way off, from a technological standpoint, so interim investment will be required in many cases to keep up with regulatory demands. As such, firms should look to embrace the concept of 'integrated surveillance' and find the point at which investing in streamlining processes and aggregating data to gain a comprehensive view of the business does not overshoot its usefulness. However, carefully building efficiency using newer technologies to bring together more relevant datasets and improve surveillance capabilities is unlikely to be wasted effort – and might even be a step on the way towards achieving something which is closer to being fully holistic in future.