A 1LoD report

The Surveillance
LEADERS' NETWORK

FORECAST 2026
October Meeting, New York

Data, Models and the AI Tipping Point:
How Surveillance Leaders Confronted
the Industry's Most Pressing Challenges

Sponsors

BEHAVOX

Nasdaq

Data, Models and the AI Tipping Point: How Surveillance Leaders Confronted the Industry's Most Pressing Challenges

The first discussion opened with a framing exercise around the four key challenges faced by surveillance practitioners: operating model, data, technology and regulation. When the room was polled, data clearly emerged as the dominant concern, with only a light show of hands for operating model and technology, and none at all for regulation. From that point the conversation largely revolved around what "data" meant in practice for surveillance and why so many firms still struggled to get it right.

The Surveillance Leaders' Network (SLN) is a private, by-invitation-only series of meetings for senior decision-makers. Members of the SLN met in New York in October to discuss the most pressing issues in the prevention of market abuse.

Participants described data as everything from the foundations of model development to the raw material for regulatory assurance. One attendee stressed that, for surveillance, data meant having a clean, budgeted training data set and the ability to experiment reliably with accurate, complete records across time. "Data to me is a clean training set that I can trust, an environment that consistently gives me complete and accurate records, and the ability to rerun experiments on that same data, including synthetic data, whenever I need." Others highlighted that they were still earlier in the journey, with the immediate focus simply on gaining access to standardised data through architectural change and aggregation layers, rather than on advanced analytics.

There was a strong sense that operating models for data and surveillance were in flux. In several firms, supervision or surveillance teams are beneficiaries of central data transformations led by technology and enterprise data offices, rather than the primary drivers. Participants described significant investment in centralised architectures, but also regional resistance and local technology teams who did not necessarily see the benefit of global solutions. "We sit at the table as a stakeholder, but technology is driving the architecture, and we are constantly negotiating with regional teams who say this global solution is not their priority, even though we depend on it for surveillance," said one participant.

Legacy system complexity remained a significant barrier. Some institutions were moving towards consolidating trading and booking platforms to reduce hops, feeds and reconciliation points, while others were still operating dozens of systems and multiple 'band-aid' surveillance platforms that could not handle all products or venues. Even firms with the luxury of a single global order management system reported ongoing data control issues and downstream breakages when central vaults or data stores were changed. "We think having fewer booking systems should simplify our lives, but we constantly see breaks when upstream controls change; we are still chasing missing trades and reconciling inconsistent fields day after day," said one participant.

The discussion also exposed a wide maturity spread across the industry. Some organisations had long-standing central data offices, standardised controls and external consultancy-led blueprints for data governance. Others described more ad hoc environments where trade surveillance analysts still discovered missing feeds only when a regulatory enquiry arrived, and then manually chased through vendors and business lines to locate trades. The group agreed that, despite progress, many banks still relied on outdated practices and have not fully embedded consistent data lineage, completeness monitoring and product taxonomies firm-wide.

In contrast to the intensity of the data discussion, regulation is not seen as the primary driver of current surveillance priorities in the US. No one initially selected "regulation" as a top issue in the opening poll. Several participants described the current period in the United States as being framed by deregulation, with no obvious street-wide thematic sweep dominating the agenda, and behaviours and abuse typologies broadly stable. "The regulations themselves are not driving our agenda right now; the real pressure is on making sure we actually see everything, that our data coverage is complete, and that we are not missing venues, products or records that regulators will expect us to have," said one attendee. At the same time, others warned against complacency, noting that large enforcement actions often reflected investigations years in the making and that a "second wave" of fines on issues like off-channel communications was likely.

www.1LoD.com

The forward-looking part of the debate centred on artificial intelligence (AI) and new technology. Participants agreed that surveillance would increasingly involve "monitoring the machine rather than the human" with huge growth in structured and unstructured data, machine-to-machine communications and AI-generated content. This raised questions about what should count as a business record, how to protect confidentiality and need-to-know, and how to trust AI-generated outputs used in trading, marketing or client interactions. "We are heading into a model-rich environment where agents talk to agents, content is created out of nothing, and we have to decide what is a record, how long we keep it, and how we defend why a model made a particular trading decision," said one participant.

Vendors around the table described similar dynamics from their side: rapid innovation, heavy investment in cloud infrastructure to process growing volumes of trade and market data, and client demand for AI-enabled tools to support alert triage, anomaly detection and calibration. At the same time, banks' internal approval processes remain cautious, with extended evaluation cycles, evolving governance models and differing levels of AI literacy among decision-makers. "Firms want the benefits of AI quickly, but their governance is often still built for older models, so you see long checklists, multiple committees and teams trying to apply traditional model risk principles to technologies they do not fully understand," said one participant.
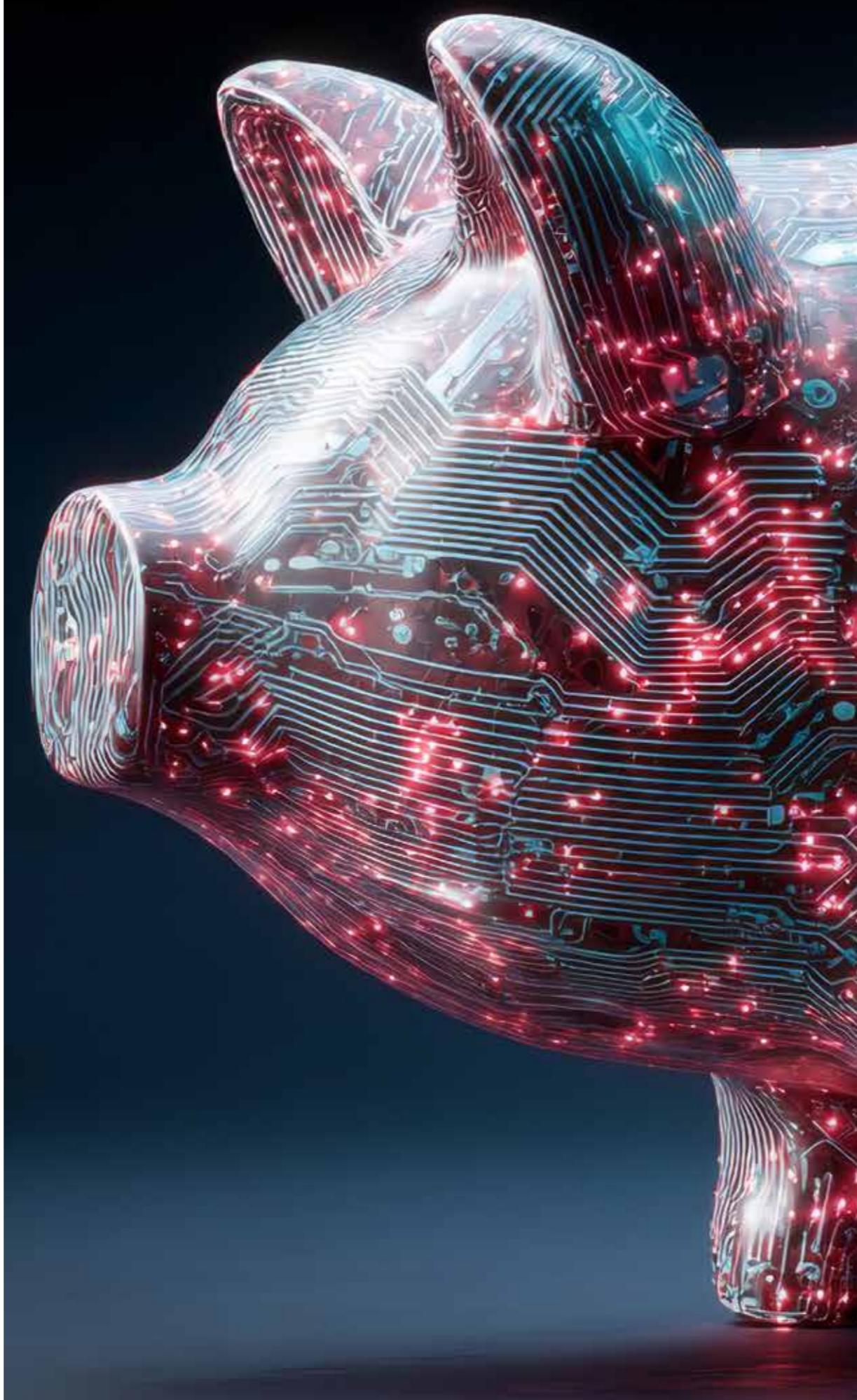
A recurring theme was the need for more agile operating models and resourcing to keep pace with technology. Participants emphasised that data scientists and quants had become a scarce, critical resource for surveillance, and that teams needed better tooling, standardised training data and repeatable pipelines. At the same time, there was frustration with model risk management functions, which were seen as both under-skilled for AI and a major bottleneck. "Model risk teams are trying to recreate outcomes as if they are pricing models, but with unstructured surveillance data that simply is not possible, and that mismatch turns necessary oversight into a brake that slows innovation to a crawl," said one participant.

The session closed with acknowledgement of the structural tension between innovation and control. Boards and fund directors were increasingly asking what their organisations were doing with AI, pushing firms to move faster. Yet participants believed that a single high-profile model failure could easily trigger a regulatory backlash and renewed defensiveness. The consensus was that surveillance leaders would need to secure better data foundations, modernise their operating models, and reshape skills and governance so that they could exploit AI and new technologies without losing sight of basic record-keeping and coverage expectations.

This information was taken from the Surveillance Leaders' Network meeting in New York on 7 October 2025.