



# Catelas Insights

Q3 2019

<b>Overview</b>	3
<b>Surveillance needs to be understood</b> From the perspective of a firm's compliance	4
<b>Questions</b> What firms have asked us	5
<b>Industry Trends</b> What firms are telling us	7
<b>In summary</b>	8

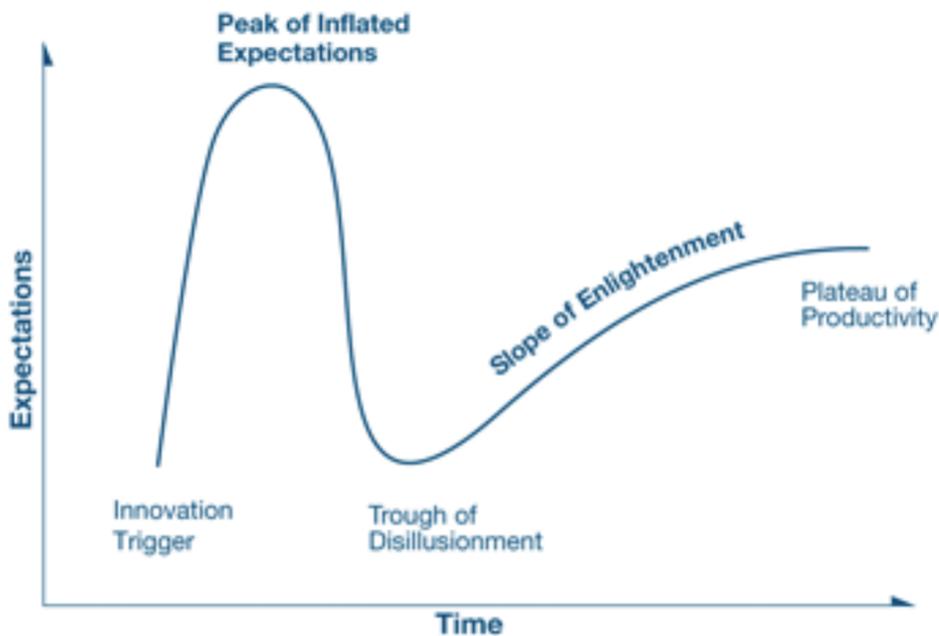
# Overview

The last five years has seen unprecedented change within the Compliance industry. Regulators have continued to become more sophisticated in their supervision and enforcement. They have invested in advanced analytics allowing them to more rapidly extend their reach – no actor in the industry is ‘outside the pale’. Examinations are more focused and deliberate in nature.

We have also seen tremendous innovation in surveillance solutions, especially around eCommunications and ‘people behavior’. However, we have also seen the typical ‘hype cycle’ created by marketeers promising ‘magic bullet’ solutions. This has led to warped expectations by both regulators and consumers of such solutions. Stories of multi-year deployments, armies of consultants, lack of control and consistency over time, abound.

The market needs to remain focused on the objective: compliance with regulations. Failure to define success, leads to solutions that will soon be obsolete themselves.

Cost of ownership of these technologies has destroyed many ROI models. The promise of process re-engineering within the framework of holistic surveillance has failed to gain widespread adoption. The industry remains highly fragmented, with vendors promising it all and, with a few exceptions, resisting to collaborate with each other.



Hype cycle

# Surveillance needs to be understood from the perspective of a firm's compliance

That program must map the regulatory framework directly to the policies that run within the surveillance tool. The reports that the surveillance tool generates must demonstrate compliance to these regulations in a highly defensible way. Full coverage is the objective and such completeness must be auditable.

## eComms Surveillance what should you expect

We have seen unprecedented innovation within eComms Surveillance. The baseline has now moved: 95% reduction in false positives is the starting point, not the end goal.

Crafting policies that target specific risks is now an everyday achievement. Our clients have seen huge success, deploying very focused effective policies covering a range of risks including insider trading, bribery, fraud, conflicts, insider risk and market manipulation across all asset classes.



### Baseline deliverable

- 95% reduction in false positives
- 100% risk coverage
- Fewer, better alerts
- Faster, more effective review



### Defensibility

- Coverage
- Audit
- Alignment with Compliance
- Reporting



### User Experience

- Ease of use
- Client control of Policy creation
- Proof of supervision
- Repeatability



### Controlling costs

- Time to value
- Fast pace of adoption
- No need for specialized skills
- No need for vendor resources

# Questions - what firms have asked us

## Can AI be defensible?

Can you audit and defend how your AI or any other advanced surveillance technology works? Can you describe it to a regulator? There can be no 'black box'.

A firm must take ownership of explaining how their surveillance works. First, you must define the intention of the technology. Then you must audit that it does what it has been designed to do.

Its performance must be both highly accurate and repeatable. For example, if you use AI to remove false positives then you need to achieve greater than 99% accuracy.

You cannot remove data from supervision, that should have been surveilled. Such errors impact your coverage and ultimately could lead to a failure to supervise.

The Catelas false positive removal process has achieved these high levels of accuracy, coverage and proof of supervision. Our machine learning models are auto-generated every day. That means it teaches itself. The client or the vendor are not needed to train it - your own data is.

The process we use is both consistent and repeatable, and describable and defensible.

## Can 100% coverage be achieved?

Is 100% coverage a requirement? Are all messages interrogated by the software?

100% coverage is achieved by defining a set of policies that address each risk scenario. Some policies are broad-based, others are focused on specific behaviors & groups.

Some policies prevent risk by uncovering 'leading indicators of risk', others look for breaches in controls or regulations.

Clients need to be on-boarded quickly. To do this we first understand a firm's risk profile and define coverage. These directly map to a firm's regulatory position.

Catelas' 100+ Policy Library is a starting point and enables us to hit the ground running. Each firm is different, and policies are edited and tested to ensure 'fit' with each client.

Out of the box internal & regulatory reporting aligns to the firm's regulatory position.

Each risk is served by surveillance policies, crafted to address risk & coverage objectives.

The end result is focused effective alerts, covering a range of risks including insider trading, bribery, fraud, conflicts, insider risk and market manipulation across all asset classes.

## The Compliance ecosystem – can it become one single ecosystem?

There is great value in integrating technology and aligning processes along the Compliance ecosystem.

Surveillance technology includes trade, personal trading, eComms, Conduct, Case Management, the archive, eDiscovery, Legal Hold.

Business processes include Front Office, Compliance, Control room, Deal Management, Audit, Security, HR, Legal.

**Aligning policy to reporting:** We work with our clients to deliver surveillance in the context of a firm's compliance program. We map the regulatory framework directly to the policies that run within the surveillance tool.

Full coverage is the objective and such completeness must be auditable.

### How can technology be consumed?

Along with the evolution of analytics & surveillance technology, we have seen the commoditization of computing resource.

Amazon's AWS and Microsoft Azure now offer an easy to use infrastructure environment that allows provisioning flexibility and cost control.

For the first time, firms have choice. Vendor technology can be deployed:

- On premise (traditional model)
- On a firm-owned cloud
- On a vendor-owned cloud



The Compliance ecosystem

A number of operating models exist.

- Client owns and operates
- Client owns and controls, but vendor operates
- Vendor owns, controls and operates

All options come with the proven security approvals of the relevant SOC 2 audit report that covers the infrastructure and associated processes. Security can be managed, and its effectiveness measured

# Industry Trends – what firms are telling us



## The Archive – a commodity

With the arrival of Microsoft's hosted SEC 17a-4 compliant archive we see major disruption in this market.

Delivered as a hosted solution, this moves the archive to commodity status and allows firms to significantly lower costs.



## 'At risk' People

Some people represent greater risk than others. Risk is linked to role and responsibility which are known, but also to behavior and activities which are unknown.

Conduct Risk scores pull these risk signals together into one place. Such people come under elevated supervision.



## Trade Surveillance integration

Firms are asking to automate the assessment of trade alerts in context of people and their comms.

Ingesting a live trade alert feed and automating the analytics around an assessment process is a quick win.



## Surveillance decoupled

Users of the near-free surveillance solution packaged with the archive are now decoupling these technologies.

Advanced surveillance brings cost savings and improved firm protection. Co-locating it with the archive no longer makes sense.



## Proof of Innocence

It is often as important to prove that nothing bad happened. Showing something is not there.

Conflict is an example of this. An investment bank must protect a client's interest. It must show that MNPI was not leaked and used against their client's interest



## The need for automation

Within a Surveillance platform like Catelas, significant value and further costs savings can be easily realized by customizing specific processes.

This is especially true in control room, conflict, information barriers, bribery and sanctions.

## In summary

A 95% reduction in false positives, very focused effective alerts, and the ability to assess alerts quickly and defensibly, is now achievable.

What makes Catelas a good fit for firms, however, is the fact that, while we offer a 100+ policy library off the shelf, we recognize that each firm's business is not the same.

We can quickly and easily modify our policies to better fit your business. This allows policies to be crafted that precisely fit what each client cares about without generating a ton of noise.

Catelas allows firms to enjoy this middle ground between ease of use and control. You can enjoy ease of use while gaining the control you need to achieve 'fit'. There are no black boxes and you don't need data scientists.

Connecting Catelas to other systems, such as trade surveillance or legal review tools is easy.

This allows your program to evolve into a more holistic solution, providing better protection while further rationalizing costs.

The balance we achieve between unsupervised automation and control over policy and audit is key to delivering a defensible framework.

Our clients are on-boarded quickly, enjoy unprecedented control and automation while enabling all the internal & regulatory reporting out of the box.

Surveillance technology can now be easily hosted in the cloud – the vendor's or a client owned environment.

We are seeing the archive being commoditized by new entrants like Office365 who are looking to become the standard for many firms – low cost, cloud based.

We are seeing the market move towards best of breed advanced surveillance technologies. This is driven by regulators who now routinely employ very advanced analytics, expanding their reach and depth of inquiry.



**Eddie Cogan** is the CEO and founder of Catelas, an advanced Surveillance & Investigation software platform, built by combining behavioral analytics and Natural Language Processing (NLP) within a machine learning framework.

Catelas' patented technology allows it to automatically map how firms do business and then to measure the risk inherent in that – whether it be insider trading, market manipulation, FCPA/bribery, fraud or insider threat.

An Engineer by training, Eddie has spent the last 20 years developing technologies that help financial services firms understand risk holistically. Mr. Cogan graduated from University College, Cork, Ireland with a degree in Electrical Engineering.



**Blake Hausladen** is VP Client Success at Catelas, where he is responsible for the success of our client deployments and for developing the product to meet current and future client needs.

Blake has over twenty five years of experience across all aspects of compliance and controls including both trade and eComms Surveillance.

Prior to joining Catelas, Blake deployed and operated Catelas technology at two firms – a large hedge fund and a large global capital markets bank. In his career, Blake has served as an RIA chief compliance officer as well as co-founder of a machine learning trade surveillance software company.