SOLUTION BRIEF

Smarsh Enterprise Conduct: Cognitive Scenarios

smarsh®

Introduction

Smarsh Enterprise Conduct reveals anomalies and trends to identify risks and opportunities in your communications data. Its ability to do so has been significantly improved with the release of Smarsh Cognitive Scenarios for supervision and surveillance workflows.

Powered by artificial intelligence (AI) and machine learning (ML), Cognitive Scenarios streamline your compliance team's review processes by dramatically reducing false positives while increasing true positives. In this brief, we explore the development methodology and review the results of a pilot program with a key customer.

The Challenge

One of the biggest challenges with today's supervision and surveillance systems is separating the real risk from the 'noise.' Review teams are required to sift through a vast and often unmanageable number of false positives to get to relevant and targeted content.

Older analytical methodologies no longer work

Traditionally, the financial services industry has relied exclusively on a lexical approach to surface risky behavior within electronic communications. Because this approach is limited to specific words and phrases, compliance teams are tasked with identifying and manually adding new terms, slang and lingo.

While this is suitable for a limited set of risk scenarios, it ultimately creates mountains of low-quality alerts while simultaneously overlooking truly risky content. This noise overloads the reviewer with the tedious task of closing false positives and can lead to increased compliance costs and significantly impact reviewer efficiency.

The Solution

Smarsh Enterprise Conduct is specifically designed to help review teams focus on real risk and eliminate noise. We do this by providing prepackaged Smarsh Scenarios for use in compliance workflows. These scenarios contain analytics to identify specific types of risk within any type of communications.

What are Smarsh Scenarios?

Smarsh Scenarios are built upon skill blocks chained together with Boolean logic and prepackaged to target a specific type of risk. Skill blocks can contain lexicons, machine learning models, natural language processing and more.

Enterprise Conduct offers two types of scenarios: Standard Scenarios and Cognitive Scenarios

Standard Scenarios

Smarsh Standard Scenarios use lexicons as the primary skill block to surface risk and have been refined as narrowly as possible to identify risk. While they are drastically improved, lexicon-based scenarios still generate a high number of alerts that must be reviewed by your compliance team.

Cognitive Scenarios

Smarsh Cognitive Scenarios contain a prepackaged machine learning model trained to identify specific behaviors that indicate risky behavior. While the ML model begins as a static model, Smarsh data scientists can continue to train and refine it with model updates. You can also use the Cognition Scenario Builder in Enterprise Conduct to augment Cognitive Scenarios with filters and additional lexicons to improve the analytic output, ensuring a targeted and refined review workflow.

Reduce false positives and increase true positives with Cognitive Scenarios

Smarsh developed Cognitive Scenarios with pre-trained ML models to give reviewers the most precise and accurate alerts and ensure a more streamlined review queue.

Building upon previous advancements, Cognitive Scenarios are the next evolution in supervision and surveillance technology with:

- **Echo cancellation** that automatically closes duplicate alerts created by email replies that include previously analyzed content
- **Augmentable scenario structure** to customize discrete alert refinement without changing the core analytics – lexical or ML
- **Filtering** to suppress alerts for specific types of communication, directionality, duplicates, near-duplicates and more

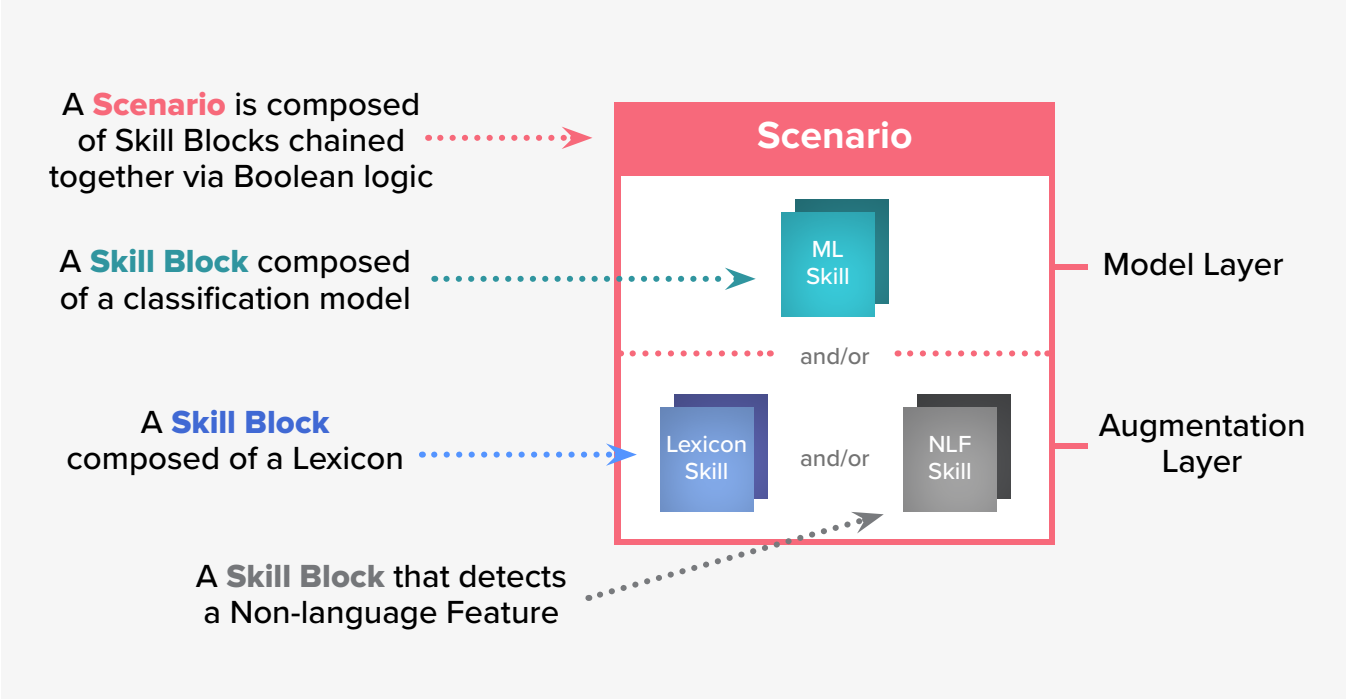
Smarsh developed these Cognitive Scenarios in close partnership with Enterprise Conduct customers using real-world data to improve and support our customers' compliance workflows. With Cognitive Scenarios, compliance teams can spend more time on true policy hits and not on low-value alerts.

Benefits of machine learning built into Cognitive Scenarios

- Detect behaviors associated with specific areas of risk
- Analyze targeted behavior more accurately
- Surface risks that slip through lexicon-only based analytics
- Provide insights into which communications or individuals are causing risk in your firm's communications

How does it work?

All prepackaged scenarios are augmentable with skill blocks to further refine the output. This gives you the flexibility to refine the output without re-training ML models.



The components of a Cognitive Scenario and how augmentation skill blocks are used.

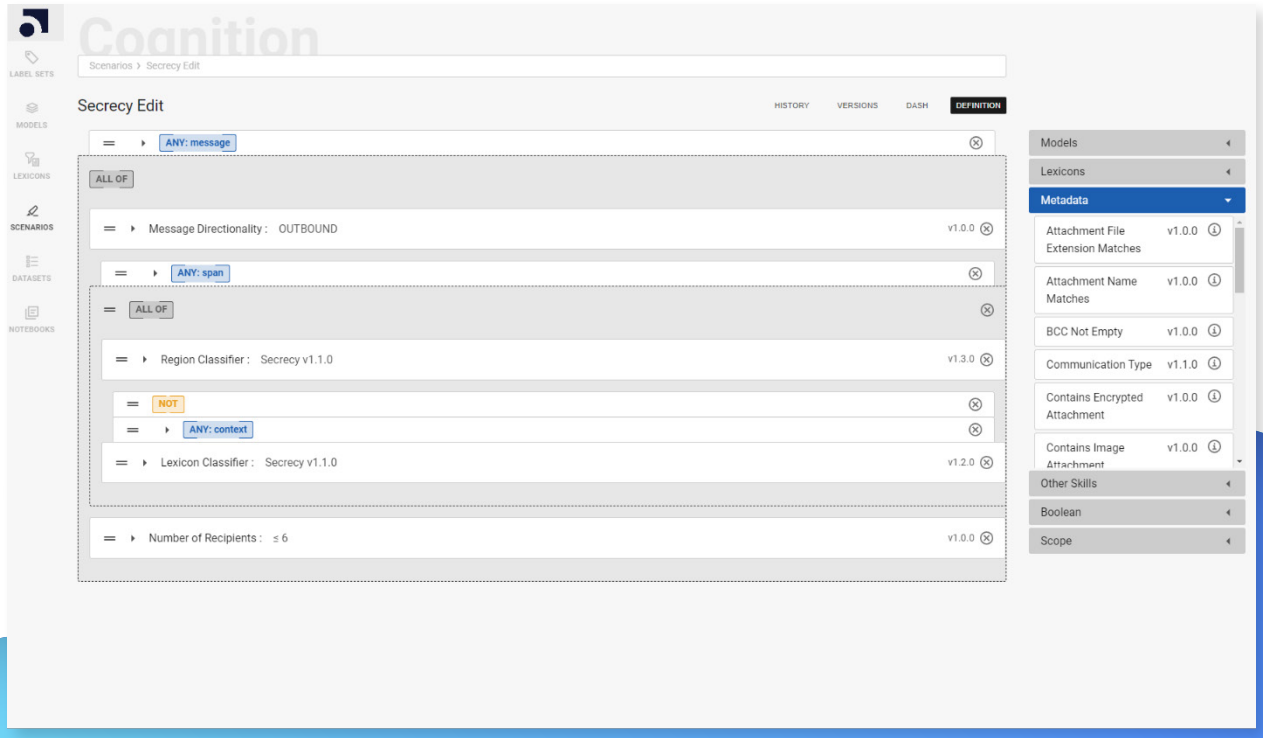
The Cognition Scenario Builder

The Cognition Scenario Builder allows you to examine and augment prepackaged scenarios and build any new scenarios.

Using Boolean logic, customers can include communications based on a wide variety of data, including:

- Message type
- Directionality
- Attachments
- And more

The flexibility of this approach allows for quick, iterative testing against a dataset to ensure that every augmentation narrows in on the targeted results. For Cognitive Scenarios that are powered by an ML model, this means you can make quick changes without re-training the model.



The Cognition Scenario Builder interface.

Why use static ML models?

Previous approaches to machine learning required a heavy lift to build, train and validate any machine learning model. This included hiring data scientists and other experts to validate both the initial approach and anytime the model is updated.

Many organizations also form model review boards that ensure the appropriate use and output of machine learning models. These boards review models every time they are re-trained to avoid model drift and other issues.

With the Smarsh approach to ML models in Cognitive Scenarios, Smarsh takes on the costs of the time-consuming, difficult work of pre-training models — so you don't have to. Pre-trained models are ready for use, enabling a faster ROI for Enterprise Conduct customers.

When Smarsh releases updates to any ML model, you can decide whether to accept or hold off upgrading based on your needs and processes. This ensures you have the best technology available with the lowest amount of risk.

Every Cognitive Scenario is fully documented with positive alert examples, solution component details, and recommendations for further augmentation if required. This documentation is available for use with internal review boards and industry regulators.

Prepackaged scenarios

Smarsh includes 50 different prepackaged scenarios ready for use by customers. All are immediately available as Standard Scenarios, and a growing number are available as Cognitive Scenarios.

Customer Mistreatment	Financial Crime	Market Conduct
• Customer complaints • Deception • Guarantees and assurances • High-pressure sales • Recommendations	• Anti-money laundering (AML) • Bribes and kickbacks	• Boasting • Change of venue • Churning • Frontrunning • Gifts and entertainment • Market manipulation • Quid pro quo • Rumor • Secrecy
Employee Conduct	**Information Security**	**Product Conduct**
• Bullying • Discrimination • Employee complaints • Inappropriate language • Outside business activity (OBA) • Payments to unregistered persons • Sexual harassment • Trading in an outside account • Conduct concerns	• Credential sharing • Circumvention of security systems • Discussion of legal proceedings • External comms with attachment • Intent to resign • PII security	• Cryptocurrency • Failed best execution • Investment advice prohibition • Suitability

Pilot program achieves 10x fewer false positives with Cognitive Scenarios

Smarsh partnered with a key global financial services client to observe and validate Cognitive Scenarios in a pilot program. We monitored the technical performance and manually reviewed all the generated alerts to determine each alert's validity.

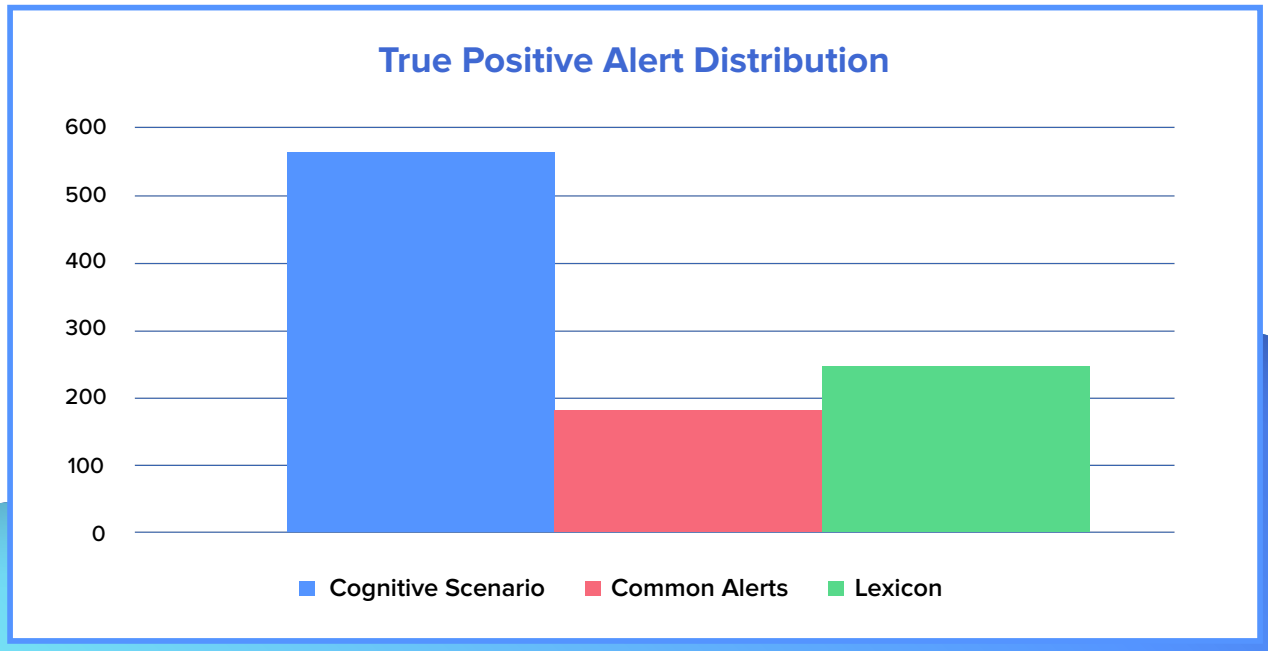
We also compared the new ML-based Cognitive Scenarios with the previous lexicon-based approach to get the complete picture of the alerts generated. Most importantly, we examined the false positive reduction rate and the increase in true positives between lexicon and ML approaches.

Key findings

While we tested all the scenarios in the pilot program, we'll focus on the Customer Complaints Scenario where we examined inbound communications for risk.

We found that implementing Cognitive Scenario:

- Significantly decreased (10x) the amount of false positive alerts when compared to a strictly lexicon-based approach
- More accurately identified risks than lexicons and surfaced more than twice (2.3x) the risk compared to a lexicon-only approach
- Reduced the volume (7.7x) of alerts needing review



Cognitive Scenario surfaces more risks than a lexicon-only approach.

Increase efficiency and productivity with Smarsh Cognitive Scenarios

Cognitive Scenarios have demonstrated remarkable improvements in supervision review in our pilot program and enabled our customer to dramatically reduce the time spent on reviewing false positives. More importantly, by revealing otherwise unseen risks, our customer is better positioned to avoid costly fines due to regulatory violations.

Smarsh continues to invest in artificial intelligence and machine learning technologies to help supervision and surveillance teams achieve greater accuracy and efficiency while reducing operational costs.

These improvements to Enterprise Conduct are a significant step in our journey to deliver a more intelligent communications data platform.

For more information about how Enterprise Conduct can help your organization or to book a demo, visit www.smarsh.com

smarsh®

Smarsh enables companies to transform oversight into foresight by surfacing business-critical signals in more than 100 digital communications channels. Regulated organizations of all sizes rely upon the Smarsh portfolio of cloud-native electronic communications capture, retention and oversight solutions to help them identify regulatory and reputational risks within their communications data before those risks become fines or headlines.

Smarsh serves a global client base spanning the top banks in North America, Europe and Asia, along with leading brokerage firms, insurers, and registered investment advisers and U.S. state and local government agencies. To discover more about the future of communications capture, archiving and oversight, visit www.smarsh.com.

Solution Brief - 11/22

1-866-762-7741 www.smarsh.com @SmarshInc SmarshInc Company/smarsh