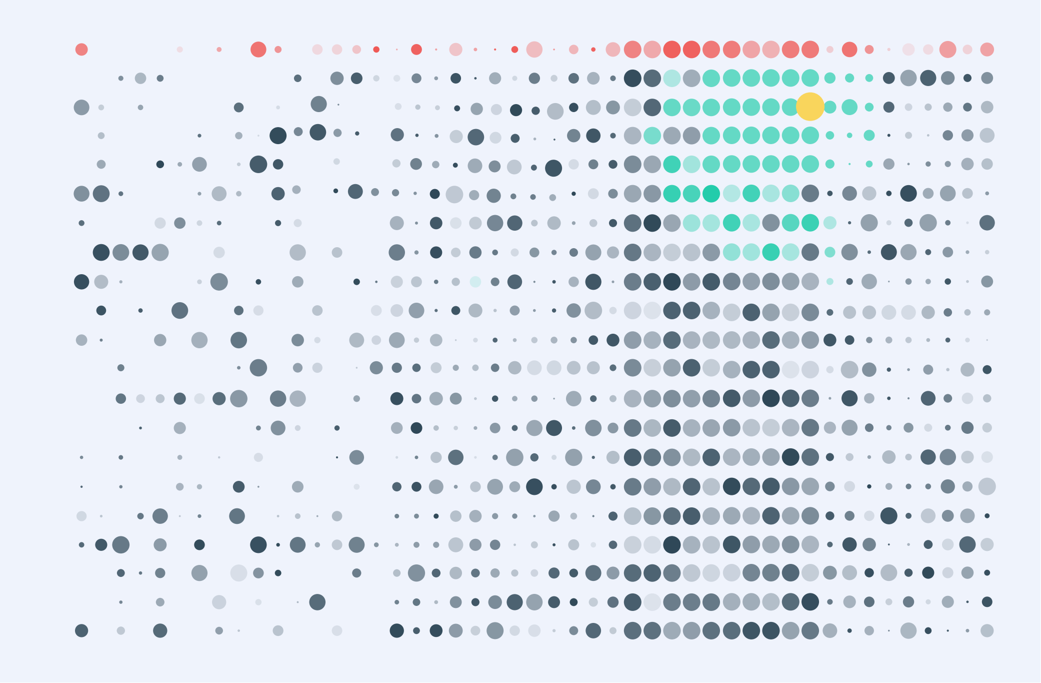


# Cogynt – A Comprehensive and Versatile Big Data Continuous Intelligence Platform

COGILITY

# Introduction

Intelligence analysts and decision makers, and by extension the enterprise, are largely behind the curve when it comes to implementing effective predictive intelligence solutions. This is due to the ever-expanding flow of data and the limitations of current IT and analytic systems. Analysts are simply overwhelmed, resulting in unquantifiable risk exposure and lost opportunity for the enterprise.

At Cogility, we regularly hear from Chief Risk Officers and operational managers that the intelligence solutions and staffing in place can, at best, adequately track only Level 1 and Level 2 risks (i.e., the highest level risks). Their concern is Level 3 and Level 4 risks: these cannot be adequately tracked with existing resources, could at any moment evolve into higher risk,and will evade detection because their current intelligence solutions and staffing don't have the level of automation or bandwidth to identify and monitor them. This challenge is common to both government and industry: it forces a conscious decision to monitor less than the entire risk surface.[1]

> "Without big data analytics, companies are blind and deaf, wandering out onto the web like deer on a freeway."
>
> GEOFFREY MOORE, AUTHOR, AND CONSULTANT

Cogility has spent more than 10 years researching and developing technology to address this critical issue. The product of this effort, Cogynt, is a continuous intelligence platform which we believe is the most effective, versatile, and affordable commercial product in the market, capable of taking on the most difficult big data intelligence challenges.

[1] Risk Surface is normally referred to in the context of cyber. In this paper, a risk surface considers all types of risk that include both technical and socio related risks.

# What is Cogynt?

Cogynt is a continuous intelligence (CI) platform that delivers contextualized predictive intelligence for analysts and decision makers. It provides event modeling, automated documentation, full provenance event detection, and complete coverage of an enterprise's risk surface.

Cogynt accomplishes this by ingesting all available data and matching this data (events)—in real time—to targeted patterns of behavior. Targeted behaviors are those impacting risk levels or identifying the emergence of opportunity. These behavioral patterns, as discussed below, are in almost all instances well known by the enterprise's subject matter experts (SMEs), and can be easily incremented or modified as new information and insights dictate. Further, Cogynt continuously assesses risk (or opportunity) for each entity or developing scenario of interest to the enterprise.

> At its core, Cogynt is a continuous intelligence platform that delivers contextualized predictive intelligence for analysts and decision makers.

During the continuous processing of data (events), if an analyst-defined threshold behavioral pattern is met, Cogynt publishes a new detection event. This instantly informs Cogynt Workstation (the visualization tool), or is communicated to the enterprise's automation platforms (e.g., SOAR[2]).

Each notification provides a wealth of information, including a quantified risk assessment with full provenance of all the underlying event history. This allows the analyst to quickly validate and understand the context of a given notification. In intelligence work, developing context is an essential, challenging, and time consuming task. Since Cogynt delivers this context on a continuous basis, precious analyst time and effort are saved. This results in timely notice, improved decision-making, and greatly expanded knowledge of the entire risk surface.

The Cogynt platform is a battle tested platform that is currently being applied in two broad market areas—insider threat and cyber threat intelligence. In both, the demand for comprehensive, timely, and actionable intelligence is critical.

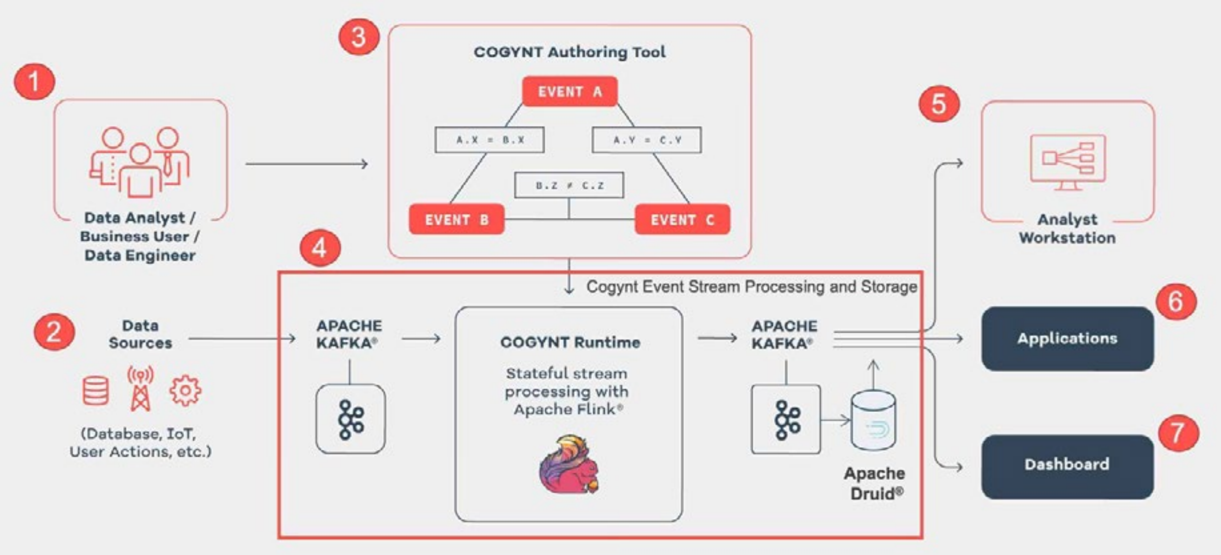
What makes the Cogynt CI platform so powerful? It's architecture, unique analytic, continuous risk assessment, agilty, zero code authoring, visualizations, and its deployment solution.

[2] SOAR: Security, Orchestration, and Response. SOAR tools allow an organization to define incident analysis and response procedures in a digital workflow format.

# Cogynt Architecture

The Cogynt CI platform is a modern Event Stream Processing analytic platform augmented with Cogility's patented real-time analytic and authoring environment, and its advanced visualization capabilities. This system was built for big data problems that can be elastically scaled within cloud environments. Today, Cogynt supports the two leading cloud service environments: Amazon Web Services (AWS) and Google Cloud Platform (GCP). Figure 1 is a logical depiction of the Cogynt CI platform, summarized in the bulleted paragraphs below:

**Figure 1** Cogynt Continuous Intelligence Platform Logical Architecture

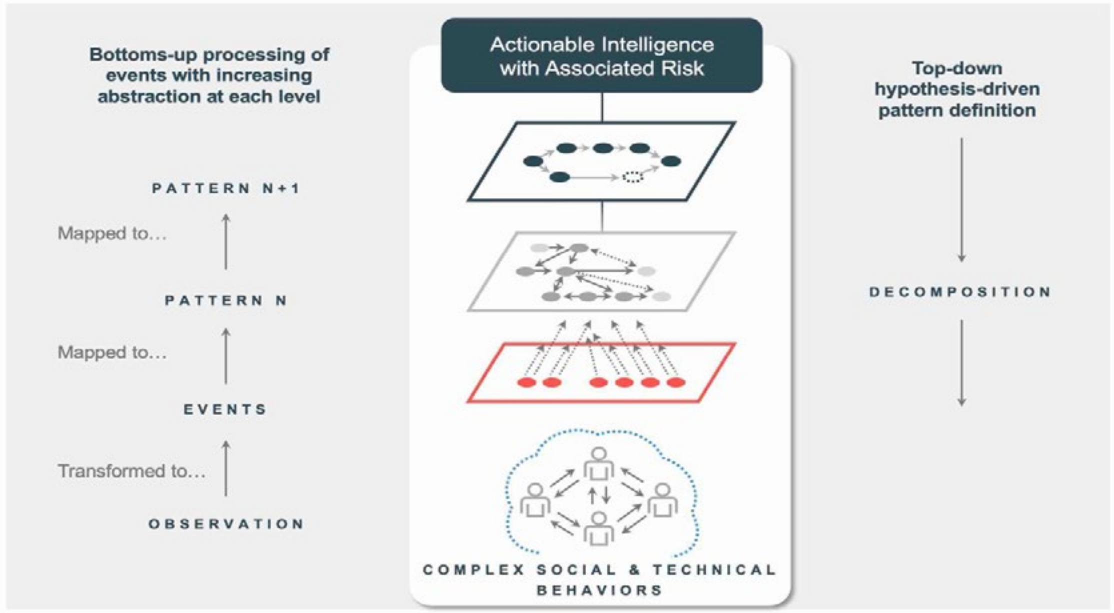


- **Data Analyst/Business User/Data Engineer** – These are the roles that define event pattens using the Cogynt Authoring tool.
- **Data Sources** – Cogynt accepts a wide range of data types and formats by leveraging Apache Kafka connectors.
- **Cogynt Authoring** – Cogynt Authoring is a tool used for authoring event patterns, computation models and risk modes. The Cogynt Authoring tool deploys these models to Apache Flink for processing.
- **Cogynt Event Stream Processing and Storage** – This includes the event stream processing software components that provide real-time processing and scalable storage for Cogynt.
- **Cogynt Analyst Workstation** – A dynamic and interactive user interface for viewing analytic results. This is the primary tool used by the analyst to review and validate system generated intelligence.
- **Applications** – Represents a notional interface to any application or system that can consume events generated from Cogynt. Cogynt is an open system and it's data can be shared with any other event driven system or application.
- **Dashboard** – The dashboard can be the Cogynt Pivot dashboard or a different dashboard depending on the customer's preference. Cogynt is an open system and can stream event data to different types of dashboards at the customer's discretion.

# Cogynt Analytic

The heart of the Cogynt CI platform is the Hierarchical Complex Event Processing (HCEP) engine, which is a real-time behavioral analytic. Figure 2 is a logical depiction of the end-to-end analytic process, as shown in the HCEP conceptual solution. The diagram illustrates how event patterns are defined from the top-down, starting with a hypothesis. The top-level event pattern is then decomposed into lower-level patterns until the user reaches the raw event level, or observation. Once the model has been established and events are flowing into the HCEP analytic engine, events are matched from the bottom up. While this process is ongoing, Cogynt is continuously assessing risk, applying a Bayesian Belief Network[3] or other weighted statistical methods, calculating a statistical likelihood of future events occurring. The event generated from this analysis is known as "actionable intelligence"—contextualized intelligence that a human can act upon. While this process is ongoing, the analyst can monitor and see the risks change over time. This allows analysts to advise decision makers of maturing risk profiles and can allow for implementation of early mitigation strategies.

**Figure 2** Logical depiction of Hierarchical Complex Event Processing


Bottoms-up processing of events with increasing abstraction at each level
PATTERN N+1
Mapped to...
PATTERN N
Mapped to...
EVENTS
Transformed to...
OBSERVATION
Actionable Intelligence with Associated Risk
COMPLEX SOCIAL & TECHNICAL BEHAVIORS
Top-down hypothesis-driven pattern definition
DECOMPOSITION

The types of big data problems HCEP is well suited to solve are typically difficult to treat with current AI/ML analytics solutions. AI/ML have proven to be very effective in detecting certain types of patterns, such as speech translation, speech recognition, facial recognition, and many others. Cogynt is most

[3] Bayesian Belief Network: https://en.wikipedia.org/wiki/Bayesian_network

Cogynt is most strongly suited where AI/ML falls short—its ability to detect and track complex patterns of behavior that evolve over long periods of time, such as human behavior, or certain sophisticated cyber-attack scenarios, such as ransomware.

strongly suited where AI/ML falls short—specifically, the ability to detect critical but infrequent events, and to track complex patterns of behavior that evolve over long periods of time. This includes areas such as human behavior, or certain sophisticated cyber-attack scenarios such as ransomware.

As stated earlier, event pattern models are created using the Cogynt Authoring tool, depicted in Figure 3, which describes the analytic process workflow.

**Figure 3**
Cogynt End to End Analytic Process and Workflow

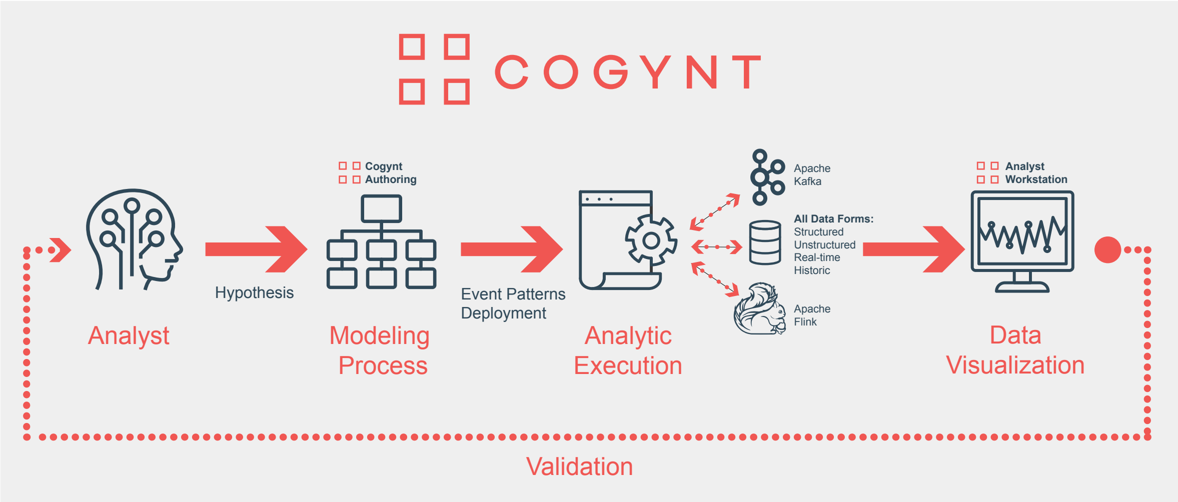


Figure 3 describes the basic Cogynt analytic process and workflow. Starting with the Authored model (using Cogynt Authoring) it is deployed by the analyst-user to Apache Flink. The HCEP event pattern model deployment converts the model into a Directed Acyclic Graph (DAG), which defines the processing data flow within Apache Flink. At execution, the data sources are piped into Apache Flink, via Apache Kafka, and the analytic results are then stored back into Apache Kafka (not shown) and displayed within the Cogynt Analyst Workstation for viewing and analysis.

This tool, which is seamlessly integrated with Apache Kafka and Flink, greatly simplifies the challenge of creating event patterns against streaming data. Its elegant modeling notation and semantics are easy to learn, enabling a novice analyst or data scientist to be productive after only a few days of training. To accelerate an enterprise's learning, Cogility also offers a three-day training class where team members develop the knowledge and skills to develop powerful event patterns and apply HCEP to solving what are typically very challenging analytic problems. The Cogynt Authoring tool is completely model based, requiring no coding. This expands the analyst user base, who traditionally have limited coding skills, thus avoiding the involvement of software engineers to implement the analytic design through long software development lifecycles.

Typically, analysts must possess detailed technical knowledge of data sources and associated schemas and collaborate with data engineers to ingest them. The Cogynt Authoring tool eases this burden with its built-in Kafka Topic schema discovery—eliminating manual schema creation and mapping to source data. Cogynt Authoring tool and analytic process also handles changes elegantly. Jeremy Turner, an experienced intelligence analyst and threat hunter at Q6 Cyber, had this to say when comparing Cogynt to Apache NiFi:

> “In NiFi, adding new data sources that alter the data model and require changes to the patterns is certainly possible, however, there are limitations in the complexity of the analysis, and performing regressions on already processed data is not simple in NiFi. With Cogynt, once a desired event pattern is produced, it is also very easy to integrate a new data element, no reindexing/recycle of the ETL, no schemas to update, no code required.”

# Cogynt Visualization Tools

## Cogynt Analyst Workstation

One of the key objectives of Cogynt is to make analysts more effective and efficient in delivering intelligence products to their stakeholders. To achieve this, Cogility has developed the Cogynt Analyst Workstation (shown in Figure 4) which provides a rich suite of analytic tools and visualizations, increasing analyst productivity, context, insight, timeliness, and overall efficiency.

> Cogynt Workstation allows the "drag and drop" of information between widgets—eliminating the need to jump between tools and applications.

The Cogynt Workstation is a modern web-based tool that is highly configurable to the analyst's preferences. It delivers a great user experience in terms of flexibility and interoperability between the tools (widgets[4]) and the ability to seamlessly perform multiple analytic functions. Cogynt Analyst Workstation allows the "drag and drop" of information objects between UI widgets—eliminating the need to jump between tools and applications. This powerful interaction allows the analyst to work at "think speed" within their workflow, providing a direct boost in analyst productivity.

For example, a notification containing critical information about an event that poses a risk can be dropped on a map widget, identifying location. The analyst may also wish to use Cogynt's auto-generated link chart, enabling the analyst to see any connections to other pertinent events or entities. Of critical importance is the drill down on the notification event, allowing the analyst to review and validate the source events that generated the notification event. Furthermore, the Cogynt Analyst Workstation facilitates a flexible workflow approach and sharing of analysis with other analysts, using "Collections" as a means of collecting data relevant to intelligence task and tagging that analysis for others to review. All user actions are also auditable, ensuring compliance with enterprise polices and regulations.

[4] Widget: A widget is a single purpose software tool among many types of single purpose tools within Cogynt Analyst Workstation. Example widgets include a search widget, notifications widget, map widget, and link analysis widget.

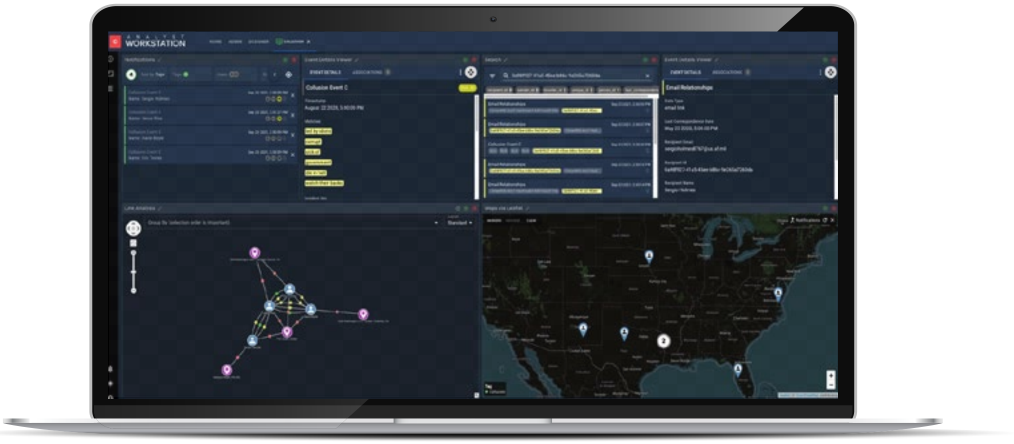


**Figure 4**
Cogynt Analyst Workstation User Interface

## Cogynt Pivot Dashboard

The Cogynt Pivot Dashboard (Figure 5) is the perfect complement to the Cogynt Analyst Workstation. It provides aggregate analysis and context for the domain understudy, while the Cogynt Analyst Workstation provides the means to perform detailed, forensic analysis of the data.

The Pivot Dashboard provides four essential functions that all enterprises need, which include:

- **Situational Awareness** – A comprehensive view of metrics and status.
- **Trend Analysis** – A determination of if and how the metric is changing over time.
- **Change Point Detection** – A significant change in a trend means that there is an underlying change in behavior of the metric being monitored, which could warrant further investigation.
- **Forecasting** – Given the trend history, this allows the analyst to forecast future trends.

The Pivot Dashboard, like the Cogynt Analyst Workstation, allows data to be visualized in real-time and can handle any scale of data. This allows analysts to explore the data easily and to create new views of various types within minutes. Figure 4 shows examples of the types of views provided by the Pivot Dashboard, including event timelines, aggregate change analysis, heatmaps, pie charts, and many others that you would normally find in a competitive BI platform.

> The Pivot Dashboard, like the Cogynt Analyst Workstation, allows data to be visualized in real-time. It can handle any scale of data, allowing analysts to explore the data easily and to create new views of various types within minutes.

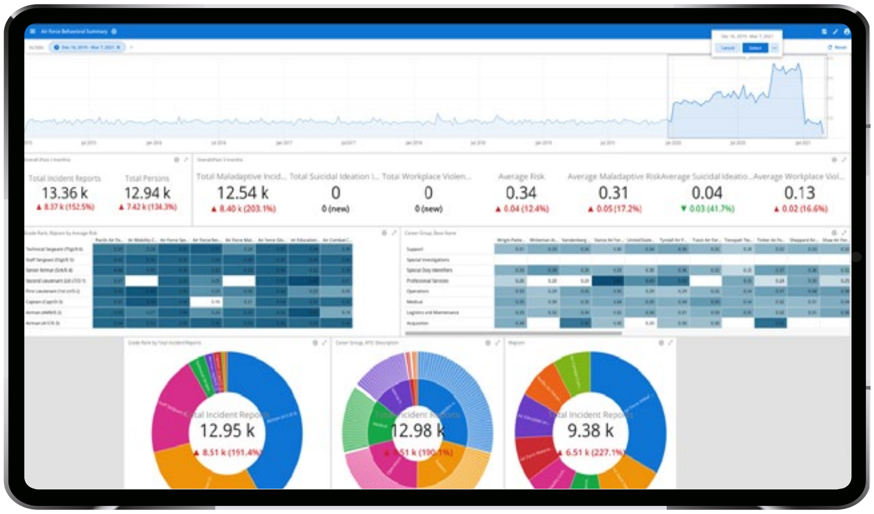
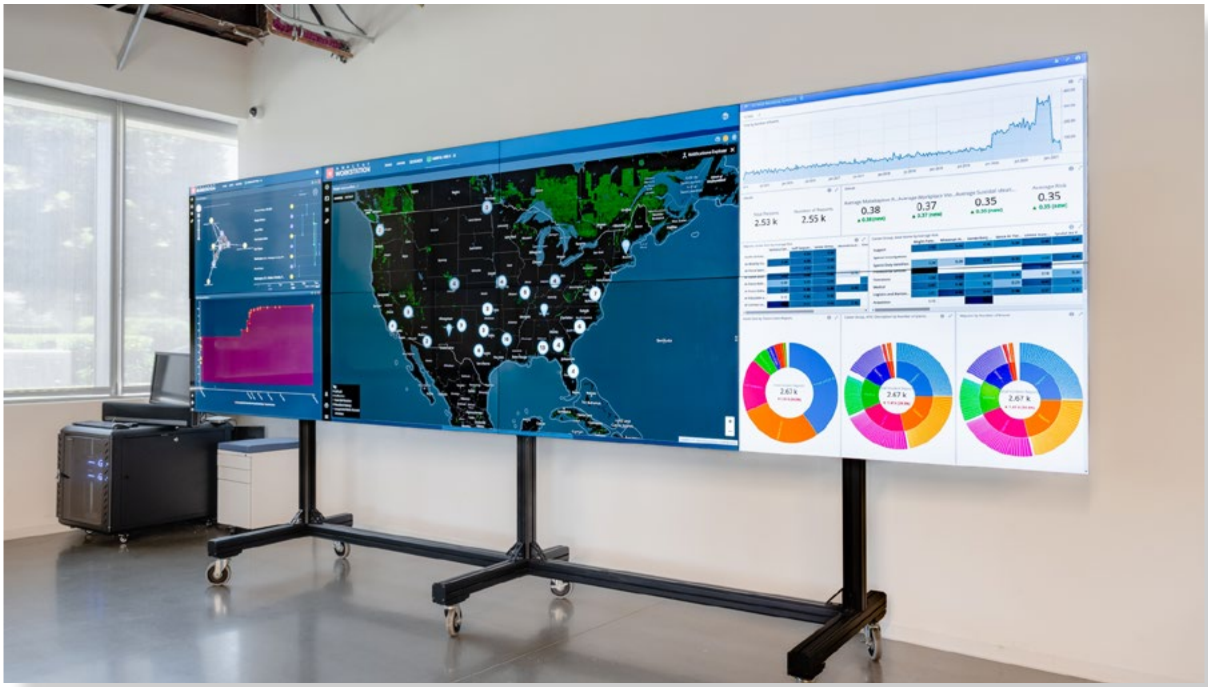


**Figure 5**
Cogynt Pivot Dashboard

## Cogynt Big Picture Wall Monitor Dashboard

To augment the Cogynt CI Platform, Cogility offers a big picture wall monitor dashboard to support operational users. This enables command and control visualization to provide shared situational awareness, support decision making, and to enhance collaboration. This big picture dashboard is being offered to customers in various formats—on multiple monitors, as shown in the following photo (Figure 6), or on a single monitor and desktop configuration.

**Figure 6**
Cogynt Big Picture Wall Monitor Dashboard



# Cogynt Deployment and Packaging Solution

Another significant benefit of the Cogynt CI platform are its deployment and packaging aspects. Cogility has fully automated the deployment of the Cogynt platform in AWS and GCP, supplemented with management tools to monitor the health of the platform. Figure 7 is a depiction of the Cogynt platform and enabling software components, including Apache Flink, Apache Kafka, Apache Druid, etc. Cogynt can be effectively managed, because the entire platform and associated software components are containerized images, orchestrated using Kubernetes. By leveraging Kubernetes, Cogynt can be centrally managed, elastically scale in the cloud, self-heal to ensure reliability and resilience, and is self-contained—it does not need to make external API calls to run. Finally, the packaging of this solution and enabling use of Kubernetes is a significant engineering achievement that allows the customer to focus on their mission without having to look under the hood.

> **By leveraging Kubernetes, Cogynt can be centrally managed, elastically scale in the cloud, self-heal to ensure reliability and resilience, and is self-contained meaning it does not need to make external API calls to run.**

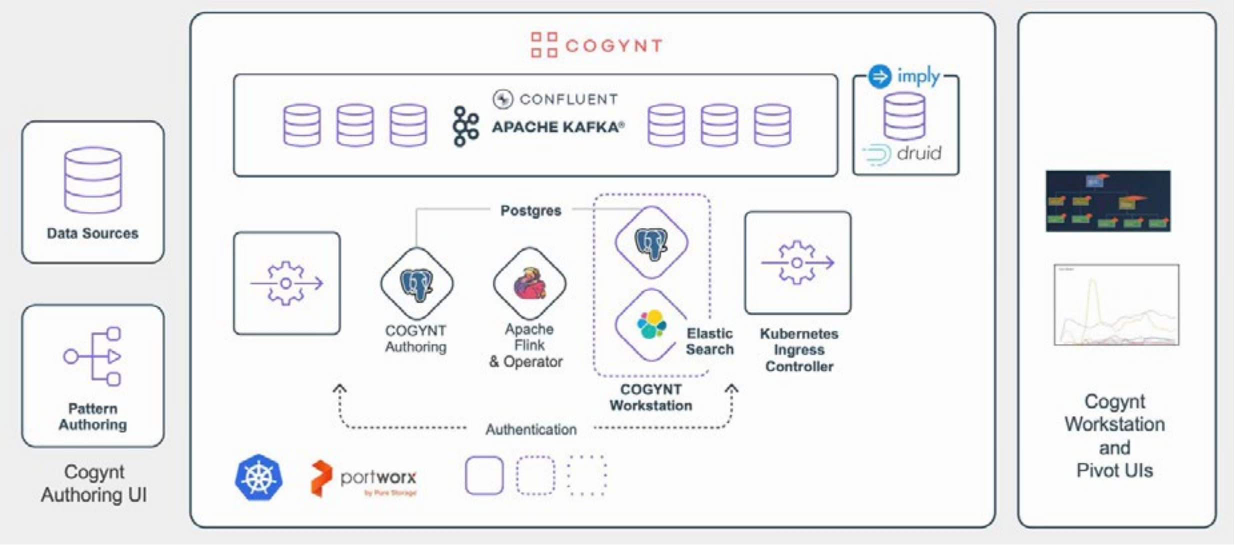


**Figure 7**
Cogynt CI Platform Deployment Solution

# Conclusion

Cogynt is a comprehensive and versatile big data continuous platform that allows enterprises to focus and grow their business while managing an increasing risk surface.

With Cogynt, analysts an data scientists can quickly connect to data sources and model complex event patterns within its Cogynt Authoring tool, expanding the scope of what can be monitored, gleaning more precise insight and accelerating performance speed. The Cogynt platform also publishes detection events to automation systems and contextual notifications to analysts within the Cogynt Analyst Workstation so they may in turn provide timely, high quality intelligence products to decision makers.

Cogynt makes this possible with its Event Stream Processing architecture, real-time analytic (HCEP), powerful visualizations, and a streamlined deployment and packaging solution. This is delivered to the user as a ready-to-use product that can address a wide range of applications spanning government and commercial use cases such as counter-insider threat, cyber insurance underwriting, and threat intelligence.

If you'd like to learn more about Cogynt, please contact Cogility Sales at sales@cogility.com.