

Build versus Buy Considerations for Decision Intelligence Platforms



Introduction

Enterprises can't afford to just react to complex business events, they need to be more proactive and anticipate upcoming threats or opportunities. Given the complex interaction of threats consisting of people, behavior, geo-political risk, market changes, weather, logistics, etc., no one person or even a team can process and devise coherent risk mitigation strategies, collaborate on key decision factors, and rapidly execute on plans without a continuous intelligence capability. To address this challenge, the Decision Intelligence Platform (DIP) is a new class of decision support automation that offers unparalleled performance in providing real-time streaming analytics solutions that will greatly increase the decision makers' situation awareness and reduce the latency of highly informed decisions. Benefits to the enterprise from the use of continuous intelligence applications that leverage this class of technical capabilities include improved operational effectiveness and mission competitiveness. Furthermore, the use of DIPs in combination with commercial cloud infrastructure, such as Amazon Web Services (AWS), allows organizations to scale to any data and intelligence challenge.

When organizations seek to upgrade their existing decision support/continuous decision intelligence applications — for example moving away from query-based analytics to stream based analytics — they are confronted with a dizzying array of technology choices that include open-source software (OSS), such as is available through The Apache Foundation Project, specialized enabling technologies, such as virtual memory management (e.g., Portworx), and custom development. All this must be integrated into a viable, scalable, and robust event-based processing architecture that supports the organization's mission needs. The availability of OSS stream analytic offerings, and the free use of the software, may seem like a free lunch on the surface, but it is far from it. Many organizations have strong technology acumen in query-based technology implementations, but even then, developing a DIP often requires a steep learning curve. This paper highlights potential challenges in operationalizing a custom DIP architecture and discusses how the Coglynt™ DIP platform handles the largest and most complex decision support workloads while offering highly effective, versatile, and proven continuous intelligence capabilities.

What is a DIP?

From a high-level perspective, as shown in Figure 1, a DIP comprises five essential elements: event stream processing, real-time analytics, decision support and business process Integration, and the human as a central element. These identified elements offer a synergistic solution that allows organizations to fully realize continuous decision intelligence.

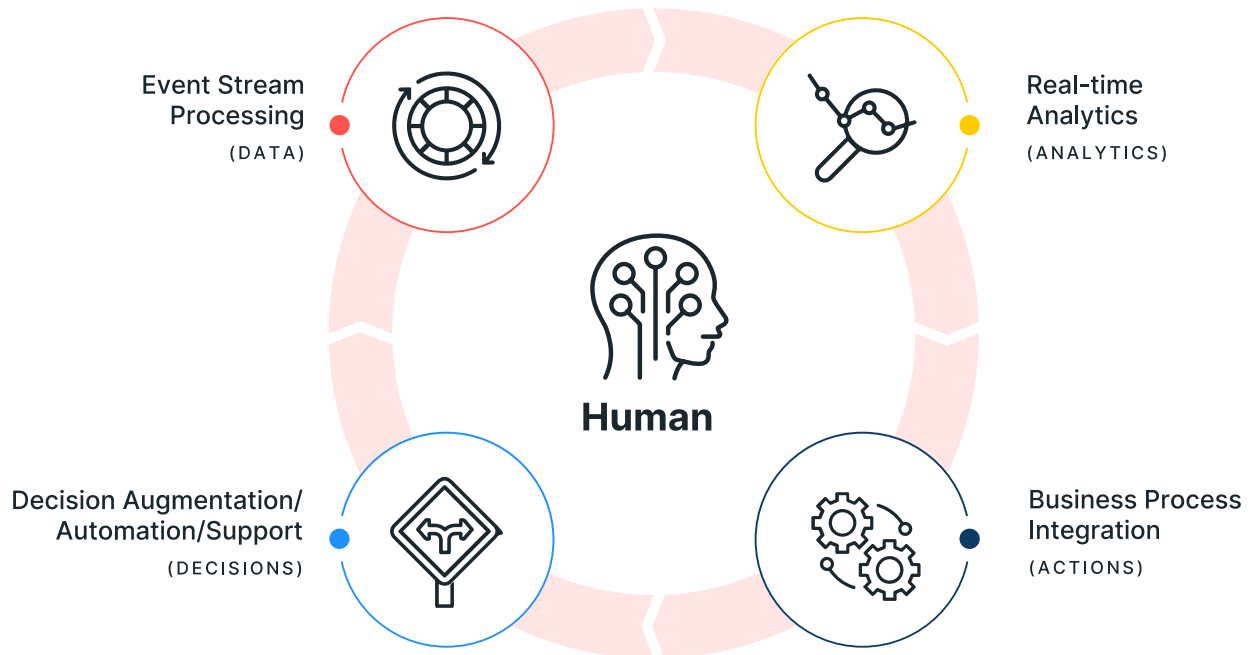


Figure 1 Decision Intelligence Platform Framework

Capabilities provided by these five essential DIP elements are:

- **Event Stream Processing** are software systems that perform real-time or near-real-time calculations on event data “in motion”. Data sources can be structured, unstructured and can be processed real-time or batch.
- **Real-time Analytics** transforms data into meaningful insights in real-time. The application of Expert AI/ML and CEP (complex event processing) are common analytic methods for “data in motion” stream analytics, as well as the emerging use of Gen AI LLMs.

These identified DIP elements offer a synergistic solution that allows organizations to fully realize continuous intelligence.

- **Decision Support** provides effective situational awareness, automated notifications, event validation, and workflow support.
- **Business Process Integration** allows for other systems and applications to be easily integrated.
- **Accounting for Human factors** to ensure the users (analysts and decision makers) are effective and efficient in performing their tasks. This is achieved through a combination of automation and intuitive, easy to use analysis tools that eliminates low-level and less productive tasking — allowing the analyst to spend more time on what is important.

Technical Considerations in Developing a DIP

An organization wishing to build a custom event-based architecture will have to make many trade-offs to find the right technical fit for their particular decision intelligence application. This requires a very experienced team capable of integrating, managing, and maintaining multiple technologies including open-source software, licensed software, real-time processing infrastructure, and custom software development to achieve the desired DIP architecture. A full IT team is needed to deliver and maintain a viable DIP—this requires product manager(s), developers, DevOps engineers, QA engineers, and technical writers, as well as mature Decision Integration and Continuous Development (DI/CD) processes and distributed cloud resource management processes. To fully realize and justify the use of DIP, the architecture and support team must provide an order of magnitude improvement in continuous intelligence application delivery, performance, analytic efficiency, and effectiveness. The sum of the parts must yield agility, resilience, scalability, ease of use, deployment, and management advantages over current query based analytic solutions.

An organization wishing to build a custom event-based architecture will have to make many trade-offs to find the right technical fit for their particular decision intelligence application.

All the above considerations factor into the design and implementation of a DIP that will support developing and enhancing an organization's continuous intelligence applications. After a DIP is deployed and operationalized, it needs an experienced team of data engineers, data scientists and DevOps engineers to ensure the DIP adapts to the changing analytic and intelligence requirements of the organization. The bottom line is that developing and implementing a modern DIP is a major technical challenge. Organizations that seek to build DIP architecture for real-time analytics to improve decision making should strongly consider the technical, operational, schedule, and cost risks that come with such an endeavor. Therefore, organizations that are looking to realize the advantages of DIPs for decision intelligence applications should consider vendors who can deliver and support a proven, agile DIP solution versus attempting to build the architecture on their own.

The tables below exemplify the technical and non-technical considerations in developing and supporting a DIP. The highlight (bold and italics) options are among the choices that Cogility has made that we believe best suits the Coglynt DIP capabilities to efficiently deliver continuous decision intelligence.

Event Stream Processing Capabilities	Example Technology Options
Event Stream Processing	Apache Kafka , Apache Pulsar, RedPanda, AWS Kinesis, Google Pub/Sub
Real-Time Streaming Analytics	Apache Flink , Apache Spark, Apache Storm, TIBCO Streambase
Stream Storage	Apache Pinot , Apache Druid, Open Search

Event Stream Processing Analytic Methods	Example Analytic Method Options
Generative AI Large Language Models (LLMs)	AWS Bedrock , Open AI ChatGPT, Meta Llama,
Machine Learning	Pytorch, TensorFlow,
Complex Event Processing and Rules Engines	Cogility Hierarchical Complex Event Processing (HCEP) , TIBCO Spotfire, Apache Pulsar, Esper, IBM Event Automation

URP Enabling Technical Elements	Example Technology Options
Container Orchestration	Kubernetes , Docker Swarm
Virtual Memory Management	Portworx , Trillo, Robin
Infrastructure as Code	Terraform , Ansible
Secrets Management	Hashicorp Vault
Configuration Management	ZooKeeper, RAFT
Data Storage	Apache Pinot , Apache Druid, OpenSearch , PostgreSQL , MongoDB, Oracle, AWS S3
Service Mesh	Istio , Linkerd, Consul
Application Programming Interface (API)	Custom

Human Interface Technical Elements	Human Interface Technology Options
Authoring Environments	Custom no code graphical UI , Java, Python, SQL, KSQL, IBM Event Automation
Analysis Tools	Custom no code graphical UI, COTS integrations
Decision Support	Custom, COTS integrations
Business Intelligence Dashboard	Superset , Pivot, TIBCO Spotfire, Tableau
Platform Observability	Grafana , Datadog, NewRelic, SigNoz, Kibana

Deployment and Support Options	Deployment and Support Options
Software as a Service	AWS , Azure, GCP , Oracle
Client Cloud Deployments	Gov Cloud, Virtual Private Cloud
On Premise	Client data centers: bare metal, private cloud

Platform Development & Team Collaboration Environments	Example Dev & Team Collaboration Environments
Source Code	Java, Elixir , Go, Rust, Python
QA and Testing	Playright , Jenkins
Source Control	Git: GitHub , GitLab
Vulnerability Testing	Tenable , Acunetix, Synopsys
Issue Tracking	Jira
Documentation, Training, LMS	Web and Video, Rise , Moodle, Cipher
Product Management	Atlassian

Organizations that are looking to realize the advantages of DIPs for decision intelligence applications should consider vendors who can deliver and support a proven, agile DIP solution versus attempting to build the architecture on their own.

Cogility’s DIP Offering – Cogynt

As described in the previous paragraphs, developing a DIP is a very complex undertaking that requires a seasoned software team and comprehensive (on-going) assessment of supporting technologies. Cogility has developed a modern DIP called Cogynt that has been cited in several recent Gartner publications, analyst blogs, and articles including

- Gartner (Event Stream Processing Market Guide, 2023)
- Gartner (Decision Intelligence Platform Market Guide, 2024)
- RT Insights article by Manish Devgan, Roy Schulte, and Sanjeev Mohan (April, 2024)¹.

The Cogynt DIP provides continuous decision intelligence for real-time, automated decision support that satisfies all the DIP requirements and delivers a completely integrated solution that has been proven in operations with the U.S. Government for insider threat management, and as a commercial cyber offering for Attack Surface Threat Intelligence. What these applications have in common is the need for very complex behavioral real-time analytics, massive diverse data ingest requirements, intelligence investigation, and advanced decision support to enable analysts and decision makers to effectively mitigate risks and act on opportunities. Cogility is a mature software company that has achieved this success by developing its patented, unique technologies including HCEP, continuous risk assessment, advanced lexical analysis, and integrated case workflow capabilities. These unique capabilities differentiate Cogynt from the rest of the streaming analytics and DIP market offerings. Whether applied to national security or commercial interest, Cogility can assure that Cogynt will support the most demanding continuous intelligence applications. Cogility has made the hard technical choices, and has integrated, tested, and operationalized its DIP technology stack. The table above and Figures 2 and 3 illustrate Cogility’s technology choices and proven integrations for Cogynt.

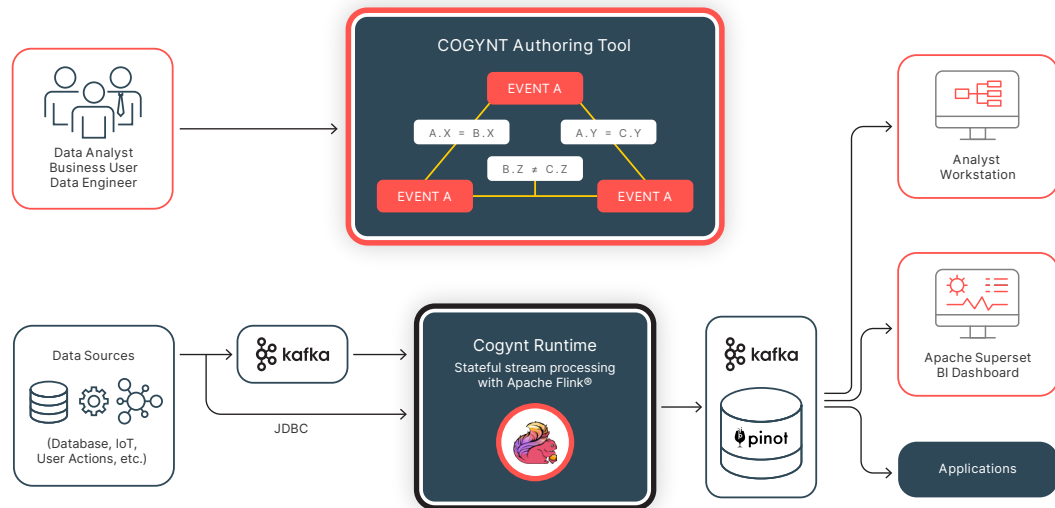


Figure 2. Cogynt DIP Logical Architecture View

1 Untangling the Streaming Landscape: The Risk of Unified Real-time Platforms

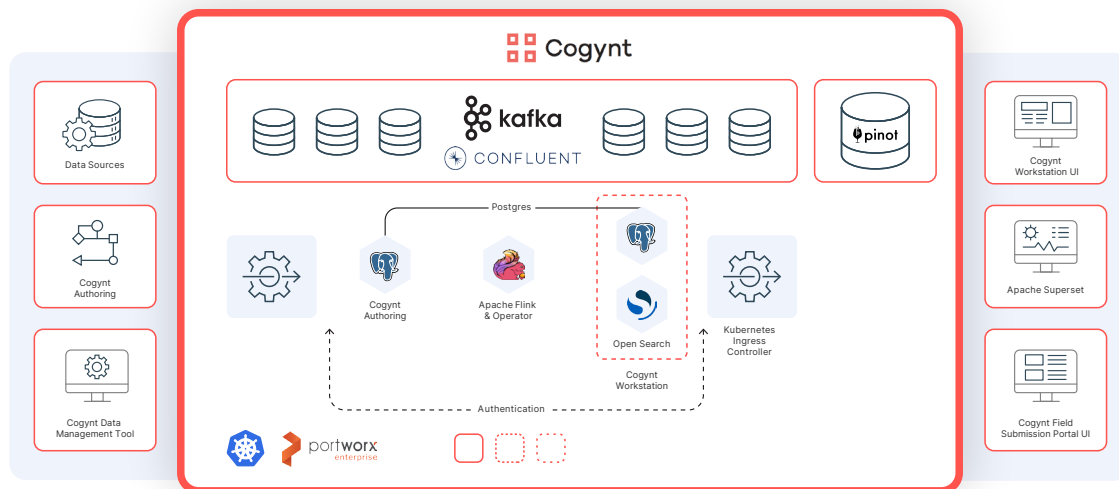


Figure 3. Cogynt DIP Deployment Architecture View

Conclusion

Organizations today are looking to improve their decision-making advantage by becoming more proactive—getting left of harm to mitigate risks—and to anticipate and act on opportunities. This requires more efficient and effective delivery of decision intelligence applications. Transforming and automating decision support operations to achieve these goals requires adept adoption of DIP technologies. Attempting to build such an architecture in-house often exceeds the capabilities of most organizations, and by doing so, introduces technical, operational, schedule, and cost risks. Instead, it makes significantly better economic and business sense for organizations to avoid the risks associated with custom technology mashups and adopt a cohesive, proven, and scalable COTS solution such as Cogility’s Cogynt. Cogynt provides a modern DIP solution that streamlines decision intelligence application delivery and on-going enhancement. Cogynt can be deployed and ready to yield decision support results within a short period of time and with less engineering overhead.

If you are interested in learning more about Cogynt, visit <https://cogility.com/platform>.



COGILITY

Visit www.cogility.com/counter-insider-threat to obtain more information and request an expert demo.

Cogility

15495 Sand Canyon Ave. #150
Irvine, CA. 92618

sales@cogility.com
+1 949.398.0015

05/25