INDUSTRY Aviation

USE-CASE Supply Chain Optimization

myngl.io

When a giant aviation company embarks on a global data-driven supply chain transformation initiative, an array of new analytics are needed. Data from across the organization is required to assess current performance and drive the optimized supply chain design. The goal is to enhance services to commercial, government and military clients worldwide while eliminating unnecessary costs, delays and related inefficiencies. The challenge was commingling the classified and sensitive data for self-service analytics.

The Problem

Commingling Raw Classified and Commercial Transaction Data

This aviation company grew by acquisition. Each business unit and subsidiary had their own supply chain systems, facilities and procedures.

Their military and government business is classified, and the supply chain data generated by such business is subject to complex granular data security and governance policies.

To enforce these rules, individual ERP deployments were used to support classified contracts. As a result, rigid data silos were spread across business units and subsidiaries.

Supply chain experts rely on industry standard metrics to benchmark performance regarding cost, agility, reliability, responsiveness, and efficiency. The same data, when analyzed, also guides the design of an consolidated, optimized and digitized global supply chain.

To compute these metrics, analysts needed to commingle millions of classified and commercial supply chain transaction records for analytics. However, the company's information security committee data commingling in systems that allow users to directly expose raw data.

The Challenge

Analyzing Commingled Data from Multiple Data Owners While Preventing Misuse

A cross functional team assigned to execute the initiative faced complex challenges that left the project stuck for 18 months.

First, the team could not remove classified or sensitive detail from any supply chain data records because doing so would generate inaccurate analytic results.

Second, the team had to guarantee that each ERP system "data owner" would be empowered to define and enforce the required granular data governance and security policies even when their data was commingled with others.

Third, the team required a single point of self-service analytic access to the commingled raw data sets. The system used could not allow raw data to be extracted or exposed in any manner that contradicted any data owner's policies.

In summary, the team needed the ability to commingle raw data and perform analytics without exposing it. They determined that none of the company's internal systems – including ERPs, enterprise data warehouses (EDW), BI systems or Hadoop data lakes – could be configured to meet these three challenges.

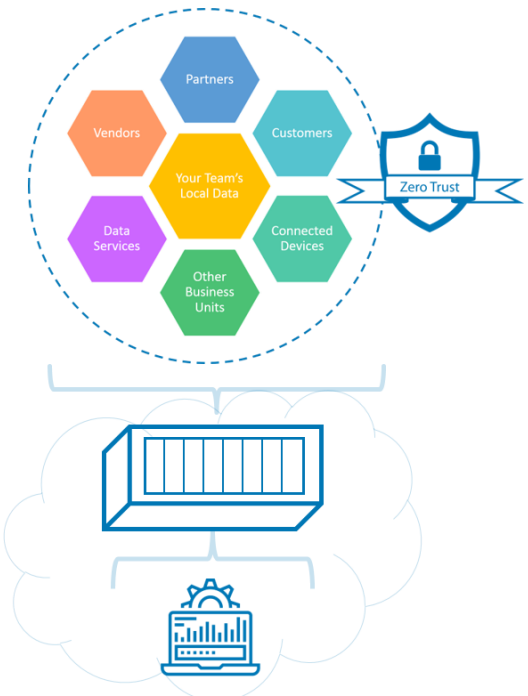
Why Myngl?

Finding an Different Approach

Our Secure Analytic Containers simplify the process of commingling raw sensitive data sets for analytics and monetization while preventing misuse. They deploy in the private or SaaS clouds making them highly scalable and easy to network together.

Unlike conventional systems, security and governance are decentralized to data owners, granting each sole control over how and by whom their data is used. We call this Self-Governing Data Security.

Zero-Trust cybersecurity processes are applied to each cell of data, making it easy for users to analyze sensitive or classified data sets without the ability to expose or extract data in unauthorized ways.



The Deployment

Leveraging Myngl's Self-Governing Data Security Mechanism

Using Secure Analytic Containers involves a simple intuitive process that begins with collaboratively defining open standard "schemas" for each shared data set.

Next, all parties agree on default "Need-to-Know" settings for every field to control how and by whom data can be used. Data owners can override any defaults at the field or cell-level of data. Once approved schemas are ingested, the container is ready to use.

Next, publishing systems move data into the Secure Analytic Container using write-only microservices. These services authenticate each system, confirms the data matches the schemas, and fuses the owner's "Need-to-Know" policy settings to each data cell. Now the data is "Self-Governing" in addition to being encrypted in motion and at rest.

The owner now solely controls how and by whom every cell of data can be used.

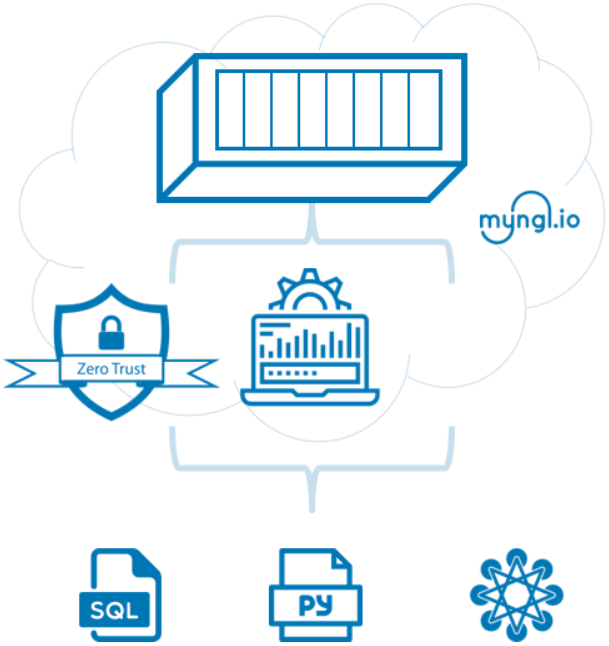
The Results

Accelerating Self-Service Analytics by 50x

Initially, 25 data "owners" were configured to publish 16 data sets. After just two weeks of post-deployment testing, the company was set to collect and analyze commingled raw data in a secure compliant self-service workflow.

Analyst used open-source web notebooks and languages in the secure analytic sandbox to address project needs. Users were blocked from directly extracting or viewing raw data in violation of Self-Governing policies. Zero-Trust microservices delivered results for use in BI dashboards, apps or automated workflows.

Once the barriers to secure data sharing were removed, the project accelerated swiftly. Access to commingled data was 50x faster than the alternative process of manual data set generation, inspection and approval.



Visit www.myngl.io to schedule a demo or contact sales@myngl.io for more information.