09/06/2022

# MDM SaaS and Secure Agent

Sourya Dass
Senior Solutions Architect, Customer Success

Informatica

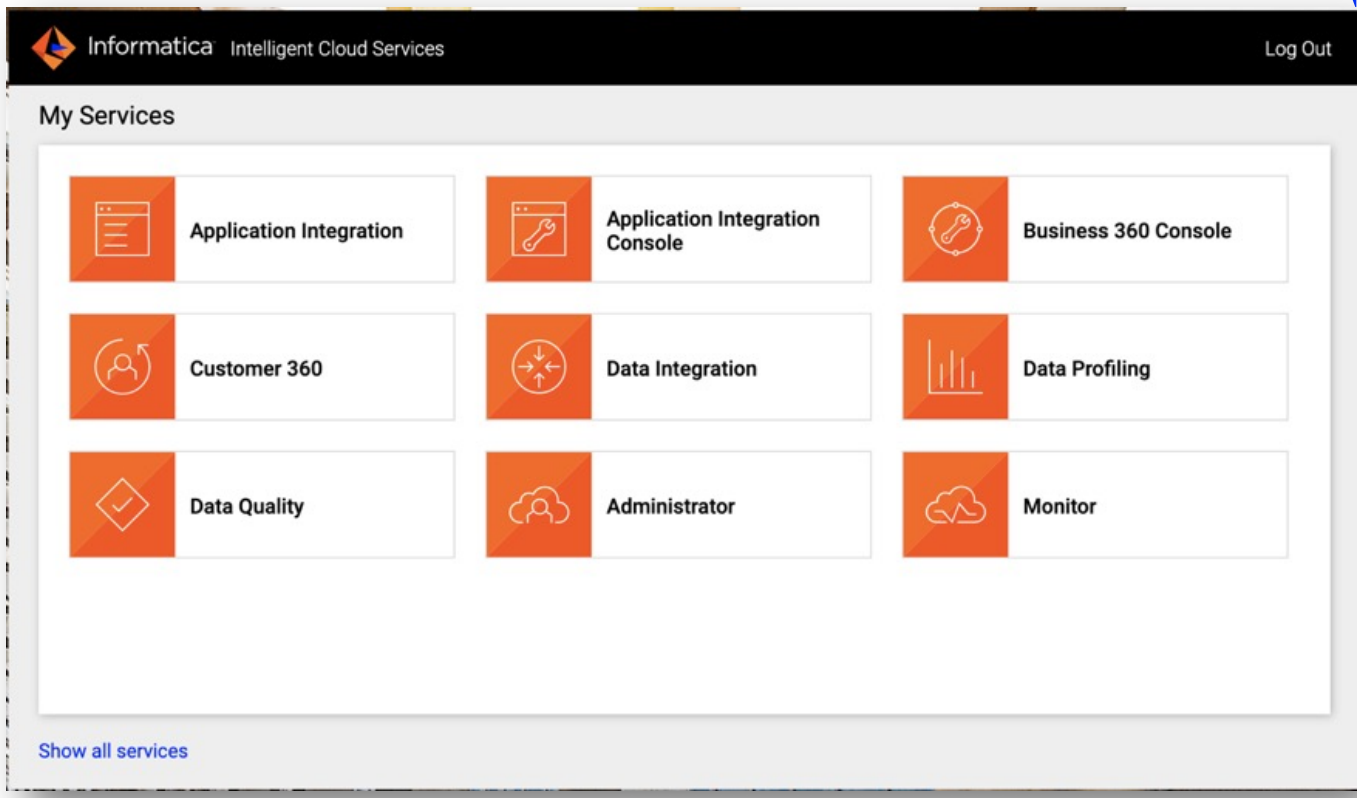
# MDM SaaS, Data Integration, Data Quality

Informatica

# What is SaaS ?

SaaS – Software as a Service is a cloud computing offering that provides users with access to a vendor's cloud-based software.

- Advantages of SaaS include:
  - Reduced time to benefit
  - Lower costs
  - Scalability and integration
  - New releases (upgrades)
  - Easy to use and perform proof-of-concepts



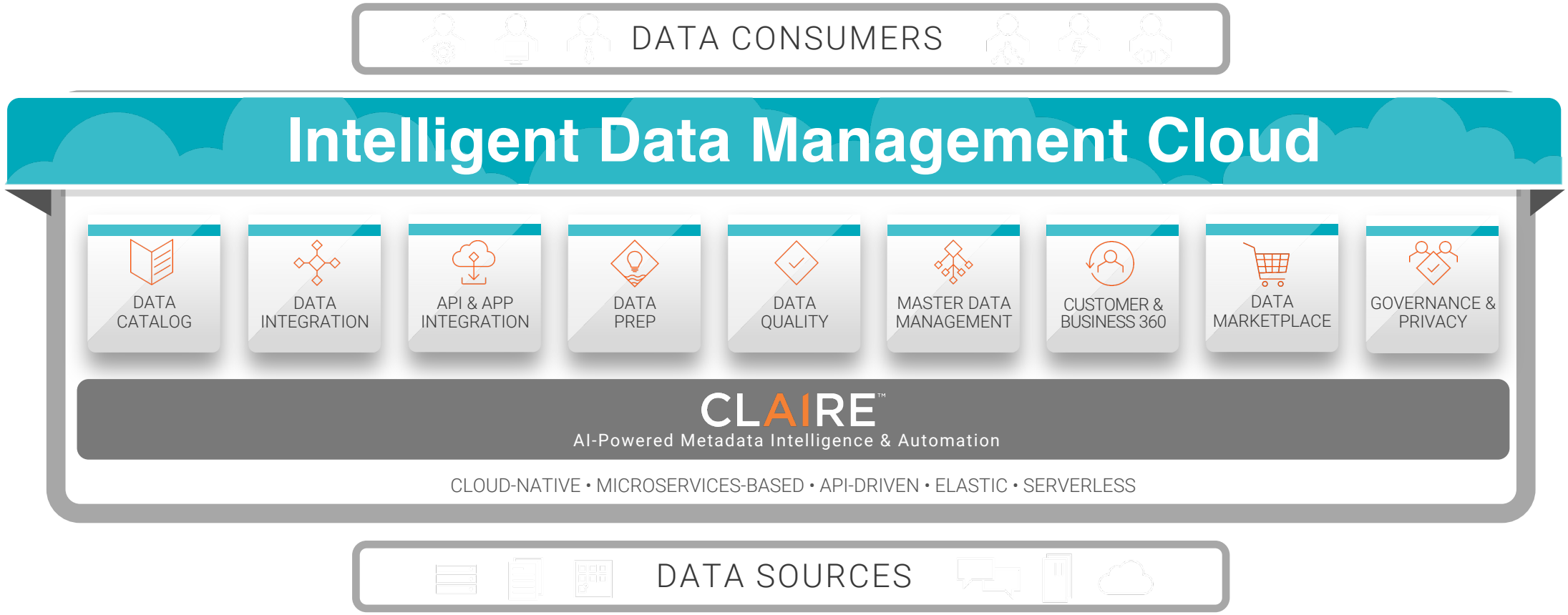




Informatica

# IDMC Platform

## IDMC combines Informatica's 260+ intelligent cloud offerings

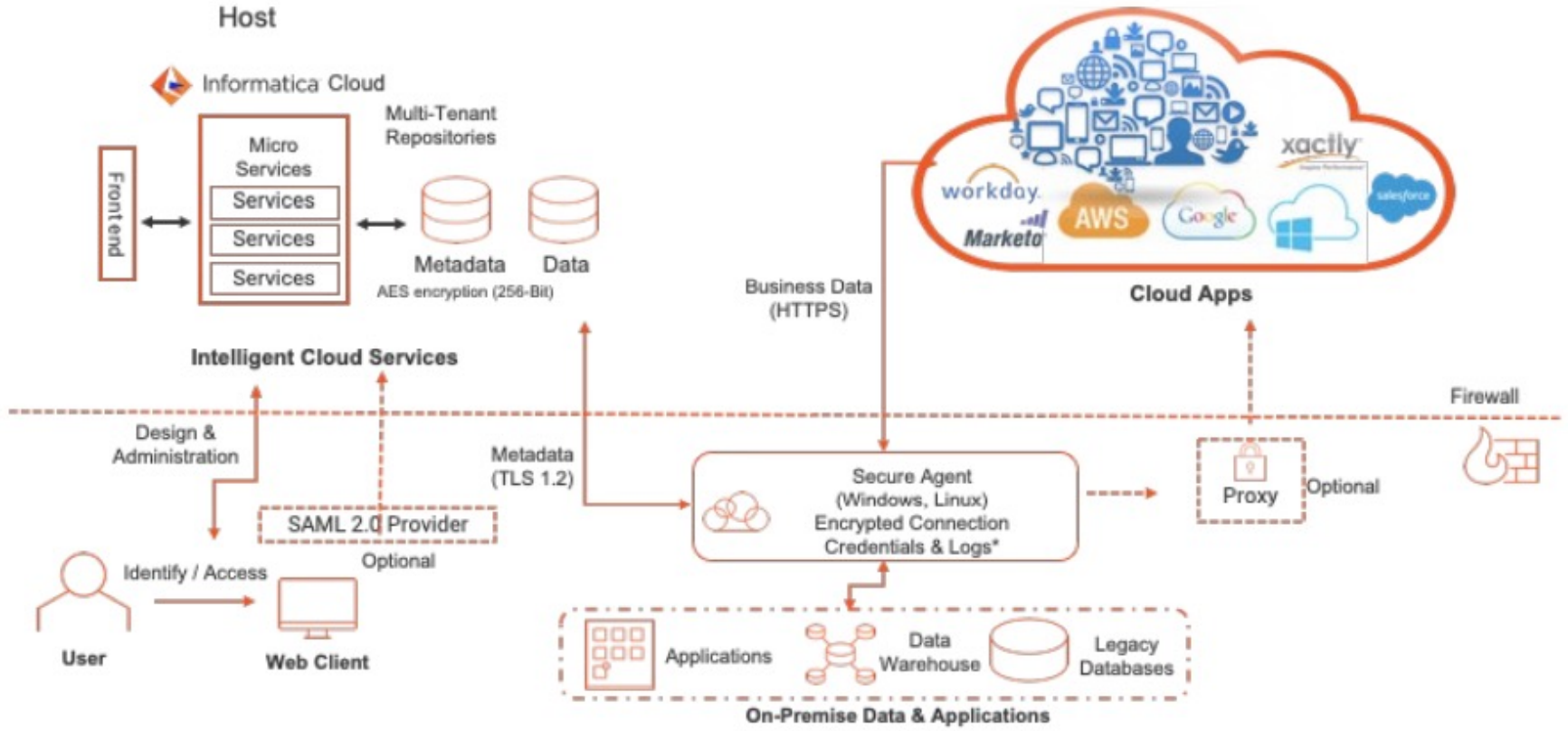






Informatica

# IDMC Architecture Components

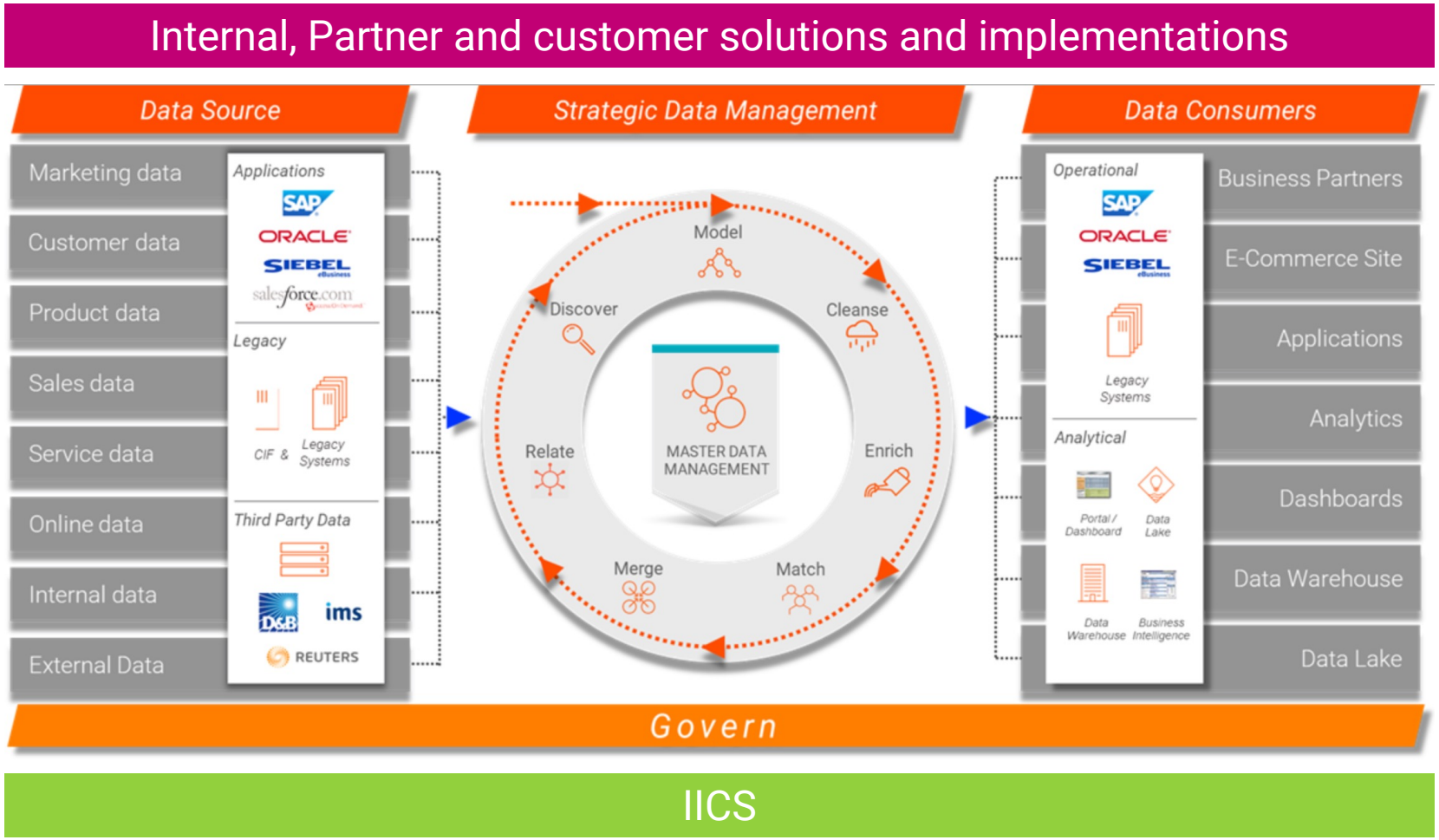






Informatica

# MDM on Cloud – user view



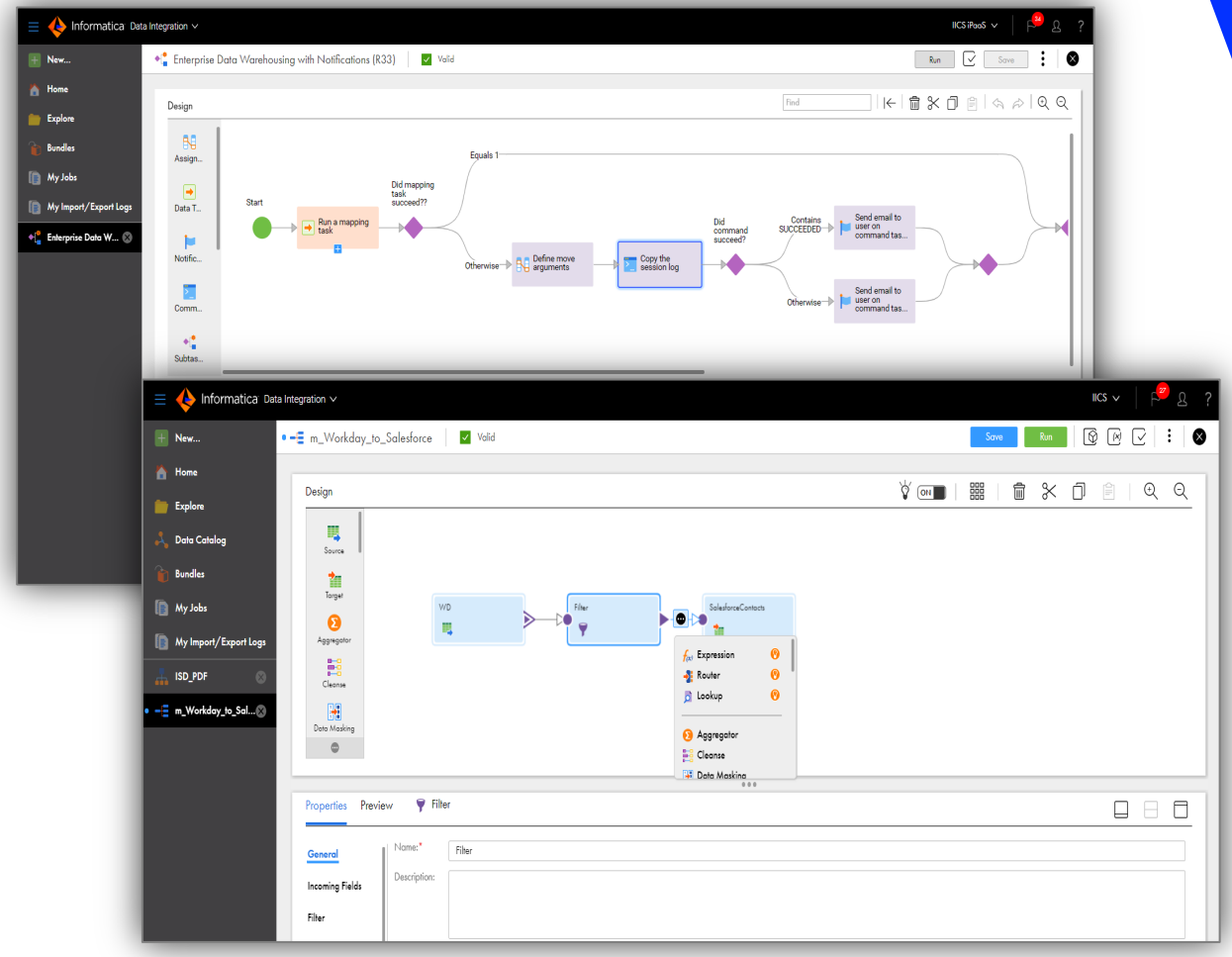





Informatica

# Cloud Data Integration

- Build simple to complex data integration loads using a mapping designer with out-of-the-box advanced data integration transformations.
- Connector support for any data type or any pattern (ETL or ELT)
- Support of Mass ingestion of any formats- files, databases, CDC or streaming
- Automatically discover any data type
- Intelligent transformation recommendation
- Serverless execution mode
- Auto tuning, auto scaling of DI jobs for greater performance & cost saving
- Heat map view of the jobs to identify critical times and peak hours for better resource planning.



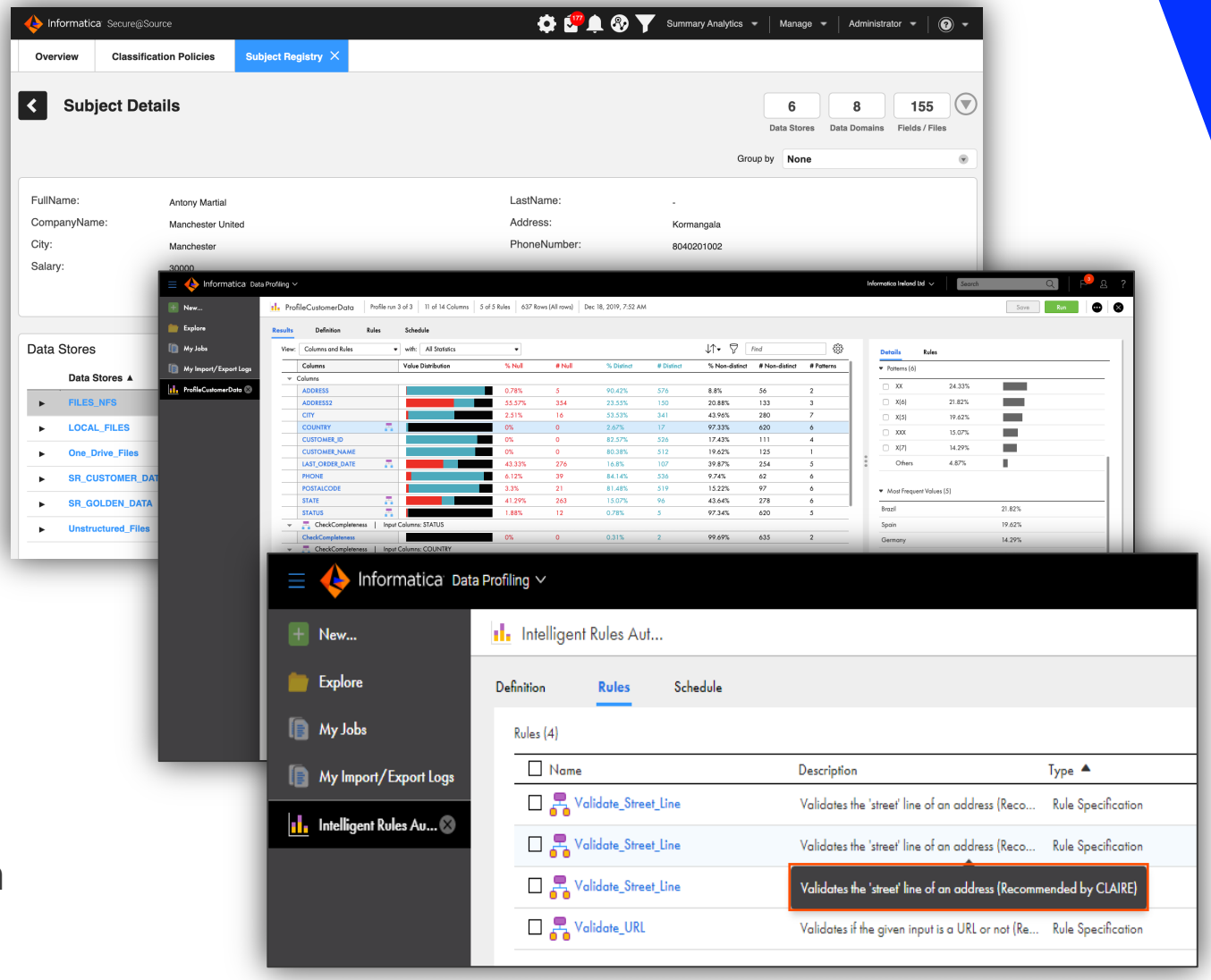





Informatica

# Cloud Data Quality

- Ensure trusted data for CDW/DL
- Empower self-service and business ownership
- Identify and prioritize data issues
- Intelligent discovery and classification of various domains including sensitive data, across structured and unstructured sources
- Intelligent rule recommendations
- Build once and re-use everywhere across cloud and on-premises
- Natural Language Processing (NLP) to auto generate data quality rules
- Automate data quality assessment and reporting across all sources
- Embed DQ processes with Cloud Data Integration



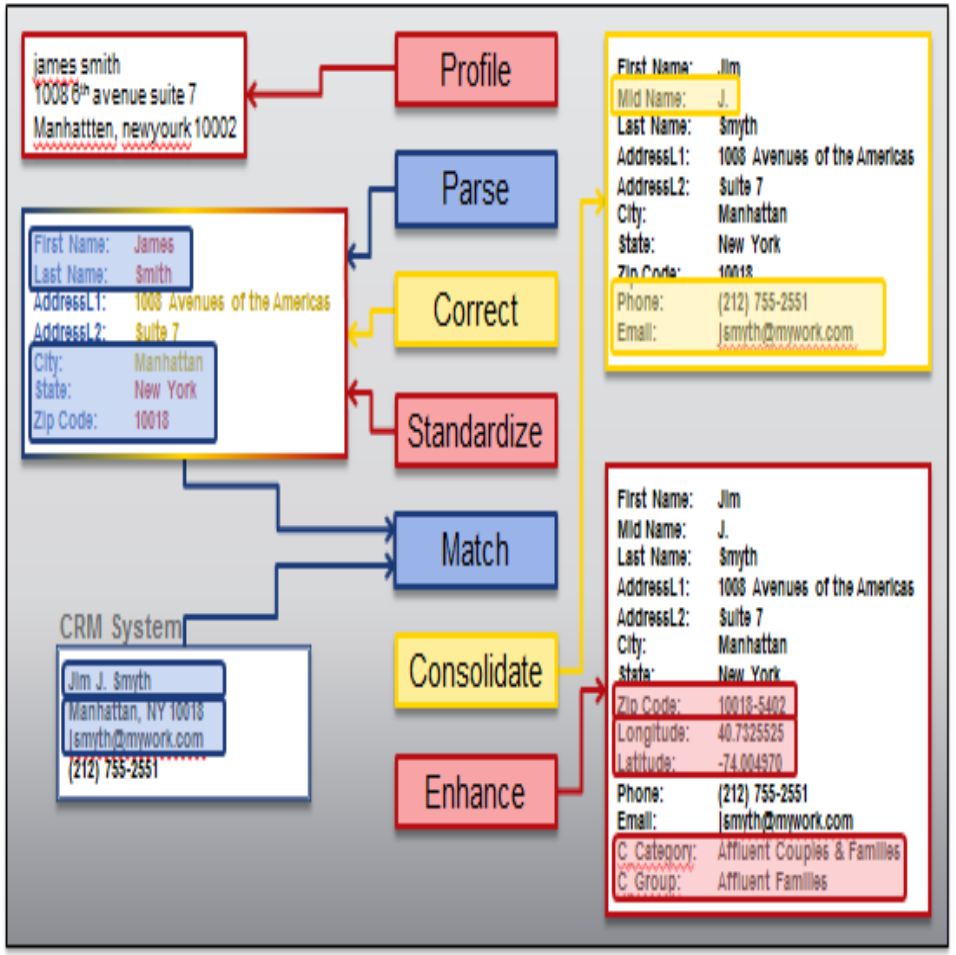





Informatica

# Six Dimensions of Data Quality

| | |
|---|---|
| Completeness | What Data is missing or unusable? |
| Conformity | What Data is stored in a non-standard format? |
| Consistency | What Data values give conflicting information? |
| Accuracy | What Data is incorrect or out of date? |
| Duplication | What Data records are duplicated? |
| Integrity | What Data is missing important relationship linkages? |







Informatica

# Data Quality Solution

Analyst &
Data Steward

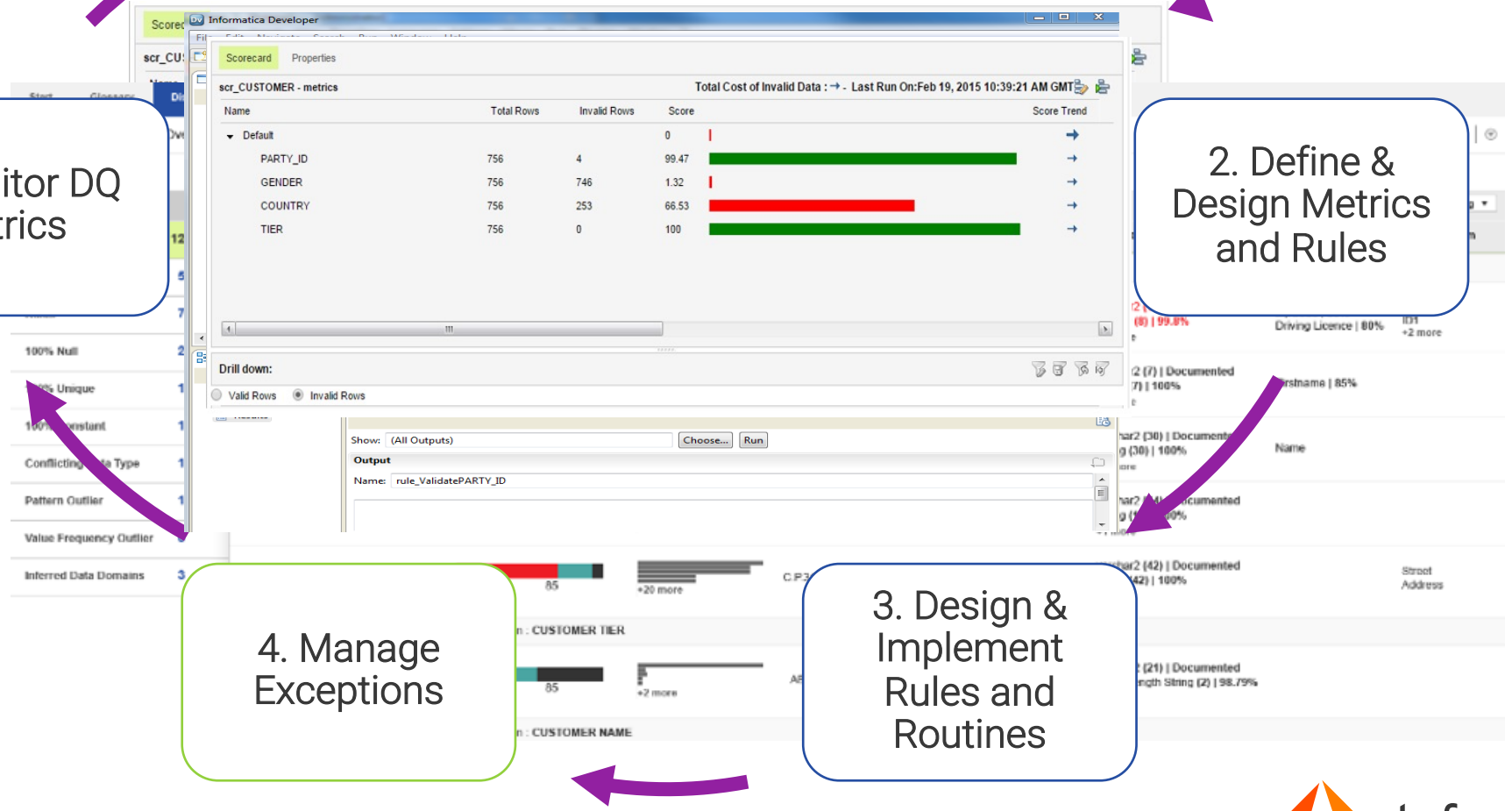
1. Profile & Discover

2. Define & Design Metrics and Rules

3. Design & Implement Rules and Routines

4. Manage Exceptions

5. Monitor DQ Metrics








Informatica

# Secure Agent

Informatica

# How Secure Agent Works

- The Informatica Cloud Secure Agent is a lightweight program that runs all tasks and enables secure communication across the firewall between your organization and Informatica Intelligent Cloud Services. When the Secure Agent runs a task, it connects to the Informatica Cloud hosting facility to access task information. It connects directly and securely to sources and targets, transfers data between them, orchestrates the flow of tasks, runs processes, and performs any additional task requirement. If the Secure Agent loses connectivity to Informatica Intelligent Cloud Services, it tries to reestablish connectivity to continue the task. If it cannot reestablish connectivity, the task fails. The Secure Agent uses pluggable microservices for data processing. For example, the Data Integration Server runs all data integration jobs, and Process Server runs application integration and process orchestration jobs. Each service has a unique set of configuration properties, such as Tomcat and Tomcat JRE settings. For more information about Secure Agent services, see Secure Agent Services. You can install and run one Secure Agent on a physical or virtual machine. After you install a Secure Agent, all users in the organization share the Secure Agent. You can configure the Secure Agent properties and move it to a different Secure Agent group. To improve scalability, you can also add multiple agents to a Secure Agent group.

# More Information on SA

- In IICS, the Secure Agent component and/or the Informatica managed cloud runtime is responsible for processing data. The Secure Agent plays a major role in securing customer data and applications and contains several security features. The Secure Agent as a platform by itself supports microservice characteristics like pluggable engines, load balancing, scalability and high availability. It consists of data integration, process server, and mass ingestion engines and connectors to external data sources to execute both batch and real-time integrations and other forms of integrations in the future The Secure Agent can be flexibly deployed on-premise or on a public cloud (AWS, Azure, etc.) by the customer to meet the customer's specific needs, or it can be managed on the IICS host by Informatica.
- The Secure Agent is attached to the customer organization at the time of its registration. The Secure Agent installer supports basic authentication and token-based authentication. When using basic authentication, the customer needs to supply the user name and password to register the agent to the customer's IICS organization. When using token-based authentication, the customer needs to supply the token granted at the time of the Secure Agent installation. Customers can also optionally configure a proxy server at the time of Secure Agent registration for its communication with cloud applications. Upon successful authentication, the Secure Agent will be attached to the customer organization. Once the Secure Agent is attached to the customer organization, it downloads binaries associated with services and connectors that the customer is licensed to and initiates the corresponding service engines. The agent also downloads any updates to engines or packages associated with the connectors during the customer subscription and service upgrade life cycle.

# Secure Agent Groups

- Secure Agent groups Use a Secure Agent group as the runtime environment when you need to access data on-premises or when you want to access data in a cloud computing services environment without using the Hosted Agent. When you select a Secure Agent group as the runtime environment for a connection or task, a Secure Agent within the group runs the tasks. Create Secure Agent groups to accomplish the following goals: Prevent the activities of one department from affecting another department. To prevent the activities of one department from impacting a different department, create separate Secure Agent groups for each department. For example, users in the sales department run 10 times as many tasks as users in the finance department, but the finance tasks are more time critical. To prevent the sales tasks from impacting the finance tasks, create separate Secure Agent groups for each department. Then assign the sales tasks to one runtime environment and the finance tasks to the other runtime environment. Separate tasks by environment. You can create different Secure Agent groups for test and production environments. When you configure a connection, you can associate it with the test or production database by choosing the appropriate Secure Agent group as the runtime environment.

- When you create a Secure Agent group, all users in the organization can select the Secure Agent group as the runtime environment. You can add and remove Secure Agents from a group. Based on your license, you can also perform the following actions: • If you have the Secure Agent Cluster license, you can add multiple agents to a Secure Agent group. • If you have the Organization Hierarchy license, you can share a Secure Agent group with your suborganizations. Note: If you use the runtime environment to run a mapping task that is based on an elastic mapping, the Secure Agent group must have only one Secure Agent. If you need to access output files on the Secure Agent machine, you can view the All Jobs page in Monitor or the My Jobs page in Data Integration to determine where a task ran.

# Secure Agent Group with Multiple SA

- When you create a Secure Agent, it is added to its own group by default. If you have the Secure Agent Cluster license, you can add multiple agents to one Secure Agent group. All agents within a group must be of the same type, for example, all agents that run within your network or all agents that run on Amazon EC2 machines. Add multiple agents to a group to achieve the following goals: Balance the workload across machines. Add multiple agents to a group to balance the distribution of tasks across machines. When the runtime environment is a Secure Agent group with multiple agents, the group dispatches tasks to the available agents in a round-robin fashion. Improve scalability for connections and tasks. When you create a connection or task, you select the runtime environment to use. If the runtime environment is a Secure Agent group with multiple agents, the tasks can run if any Secure Agent in the group is up and running.
- You do not need to change connection or task properties when you add or remove an agent or if an agent in the group stops running. When you add multiple agents to a group, ensure that all of the Secure Agents are of the same type. For example, your organization installs four Secure Agents on physical machines within your network and two Secure Agents on Amazon EC2 machines.
- You can create a Secure Agent group that contains some or all of the local agents and a different group that contains the EC2 agents. Do not create a group that contains both a local agent and an EC2 agent. If you need to access output files on the Secure Agent machine, you can view the job details to determine which Secure Agent ran the task. To view job details, open Monitor, select All Jobs, and click the job name.

# Download & Install Secure Agent

## Requirements

- Secure Agent may be installed and operated on a multi-core CPU machine with up to four (4) physical Cores (Not Logical/ vCPUs). Linux or Windows.
- Minimum of 16 GB RAM. Recommended to have up to 32 GB RAM with 8 Cores using FEP to accommodate all IICS services up and running like a process server, OI Data Collector, Mass Ingestion, common integration services, File Integration Services, etc.
- At least 250 GB disk space to run your tasks and store caches and logs with success.
- And more…Minimum requirements and best practices

## Other Considerations

- Consideration for installing extra Secure Agents in an Org:
  - Grouped: H.A./Load Balancing, Separate Memory Resources (vertical scaling)
  - Adding Cores: Fast and Parallel Jobs (Horizontal scaling)
  - Separate:  Dividing by Services, LOBs, or optimized for Source/Target
- Secure Agent Links
  - FAQs – Secure Agent Group, Cluster Server Considerations, Increase Java heap size and other memory attributes
  - Admin Guide – Secure Agent Services and Grouping Details

# Demo


Thank
you