boomi

Boomi Security and Privacy

Overview of Data Flows with Boomi

Updated November 18, 2025

Content

Background

This document describes the various data types and flows associated with customer or partner use of the Boomi Services.

Cloud Terminology

While "the cloud" has entered the mainstream business vernacular, Boomi denotes cloud terminology under the following descriptions

1. **On-Premises**

   Traditional hosted applications located in customer data centers or behind customer firewalls.

2. **Hybrid Cloud**

   Extending the application boundary where business applications run and store data on third-party cloud services, e.g., AWS, Azure, and/or Google. These applications are secured via a dedicated virtual private cloud, between the hosting provider and the customers datacenter entry point.

3. **Public Cloud**

   These are Software as a Service (SaaS) based applications hosted on third-party clouds but not a part of the IT architecture, e.g., Azure VM, or AWS Storage (S3).

4. **Private Cloud**

   A private cloud is a cloud computing environment in which a company's IT infrastructure is hosted on servers controlled and managed by the company, rather than a third-party service provider.

5. **SaaS**

   Software licensing and delivery model in which software is licensed on a subscription basis and is centrally hosted by the application vendor. E.g., Microsoft O365 for email, calendaring, or Salesforce for CRM.

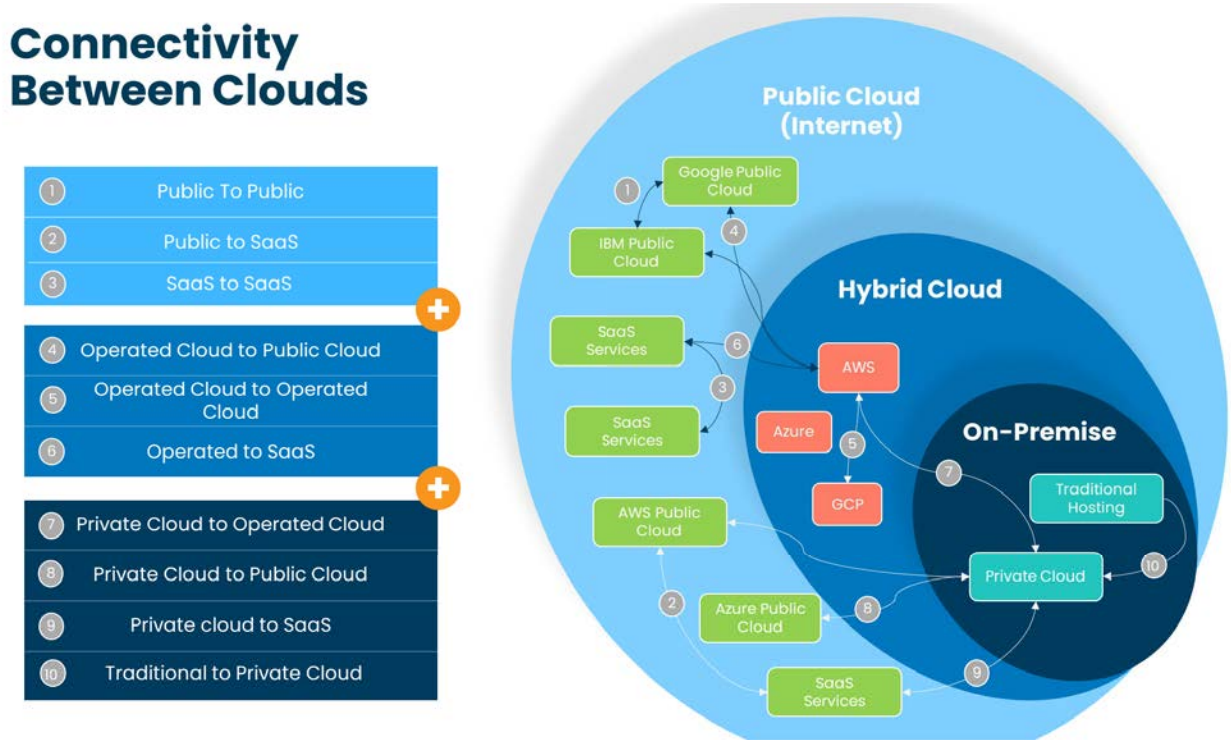

Diagram 1: Connectivity Between Clouds

Boomi Enterprise Platform Overview

The Boomi Enterprise Platform is a cloud-based integration Platform as a service (iPaas) that consists of two key parts: a web application control plane (the "Boomi Enterprise Platform") and an independent runtime engine (the "Boomi Runtime") that can be installed locally or hosted in a cloud.

The Boomi Enterprise Platform is where customers design, configure, deploy, monitor, administer, and manage their processes. Currently, Boomi serves all global customers and partners from a single Boomi Enterprise Platform, hosted in North America, in AWS (East)and is only available as a cloud-hosted service.

Once developed, processes are deployed to the Boomi Runtime for execution. The Boomi Runtime is a self-contained application that performs deployed process logic and securely connects directly to endpoint applications and data sources. The Boomi Runtime communicates with the Boomi Enterprise Platform to receive configuration updates and report the results of process executions.

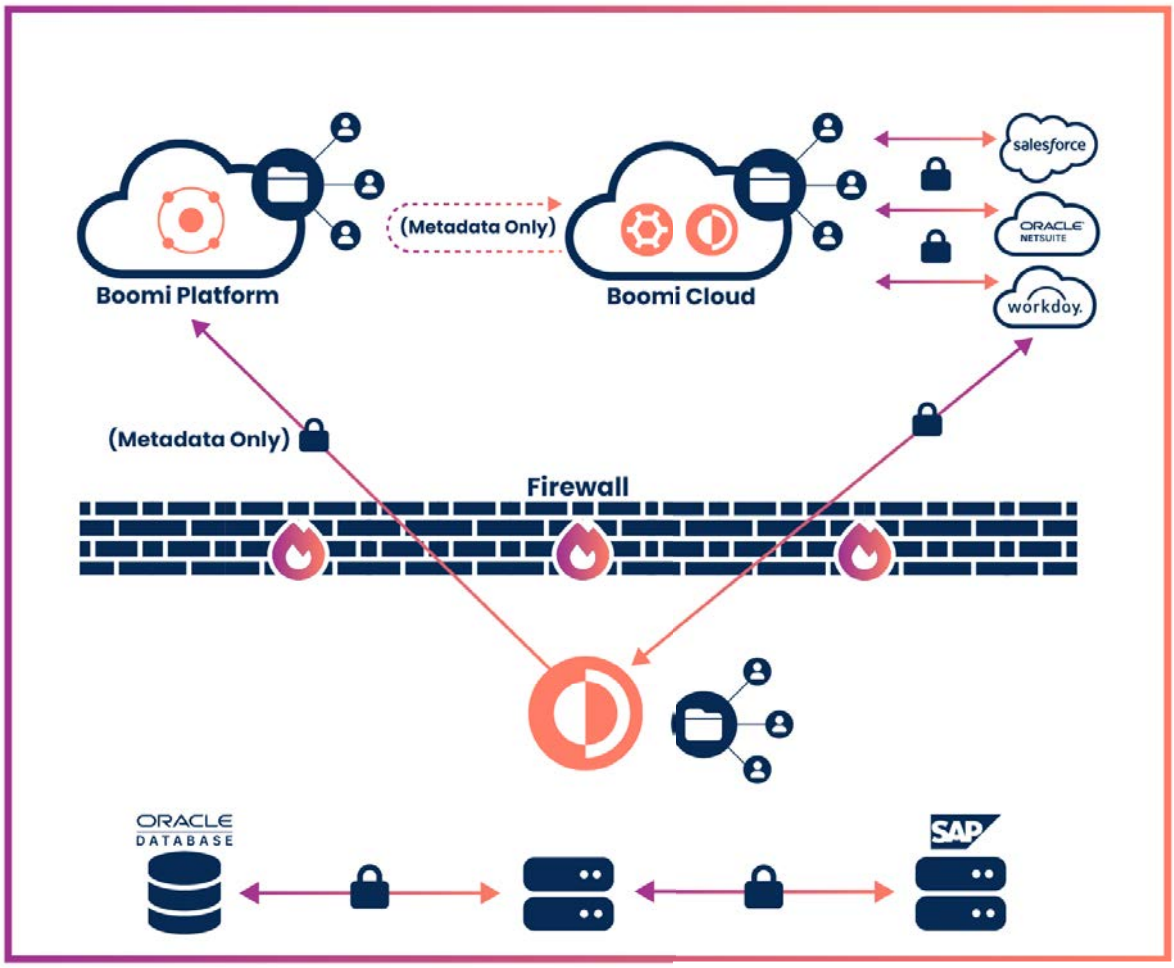

Diagram 2 – Boomi Platform Architecture

Understanding the Data Types

The following table outlines the different types of data Boomi considers as part of the Boomi Enterprise Platform service.

Data Type	Description
Boomi Enterprise Platform Metadata	Boomi Enterprise Platform *metadata* refers to data that is collected by the Boomi Services, e.g., status information, IP addresses of connected users, runtime resource data or system information. This data is collected by Boomi (as with any SaaS

	service) to better operationalize customer specific services, perform security and operations management, protect against fraudulent or illegal activity, and other purposes as set out in the product documentation. Furthermore, it allows Boomi to utilize the statistical data and information gathered during a customer's regular use of the Boomi Enterprise Platform to help us improve the overall experience.
Design Time Configuration Metadata	Design Time Configuration Metadata refers to the data that defines how the different Boomi Services are structured, connected, and managed within the Boomi Enterprise Platform. It includes the configuration and design information created when using the Boomi Enterprise Platform such as process flows, business logic, field mappings, transformation rules, connectivity details (e.g., hostnames, endpoints, and user IDs), discovered APIs, API product definitions, usage plans, and API consuming applications, and version history, for example. Design Time Configuration Metadata does not include Processed Data as described below.
Runtime Configuration Data	Runtime c*onfiguration data* refers to data and settings which can be specified for an integration runtime or API Gateway. This includes various application properties that control different aspects of the runtime engine, Java system properties as well as settings for the embedded web server and queue server.
Processed Data	*Processed data* refers to the actual business data that is processed by Boomi integration, such as data received as an incoming API or event request, or data retrieved from a database or ERP system.
Boomi Enterprise Platform Account Data	Boomi Enterprise Platform *account data* refers to an end user's credential information used to log into the Boomi Enterprise Platform. This data is encrypted and hosted in our secure datacenters (in the US).
Log Data	*Log data* refers to log information compiled from activities performed during design and management on the platform, as well as during execution on the runtime.

	• *Audit Log Data*: Captures management and account configuration activities and changes performed in the platform control plane by users (via the UI or Platform API). • *Process Execution Log Data*: Acquires the log files for each integration process execution that contains step-level behavior for troubleshooting purposes. These logs are retained according to the configurable purge schedule. • *Runtime Logs* - Various logs that capture behavior of the runtime engine itself and key components, such as the shared web server and execution workers. These logs are retained according to the configurable purge schedule.

Platform Security

As a global provider of platform based services, security is paramount to Boomi. More details on Boomi security, including relevant certifications, are available through https://boomi.com/compliance/.

The following diagram details how Boomi secures and encrypts the various types of data as described in this document both inside and outside of the Boomi Enterprise Platform.

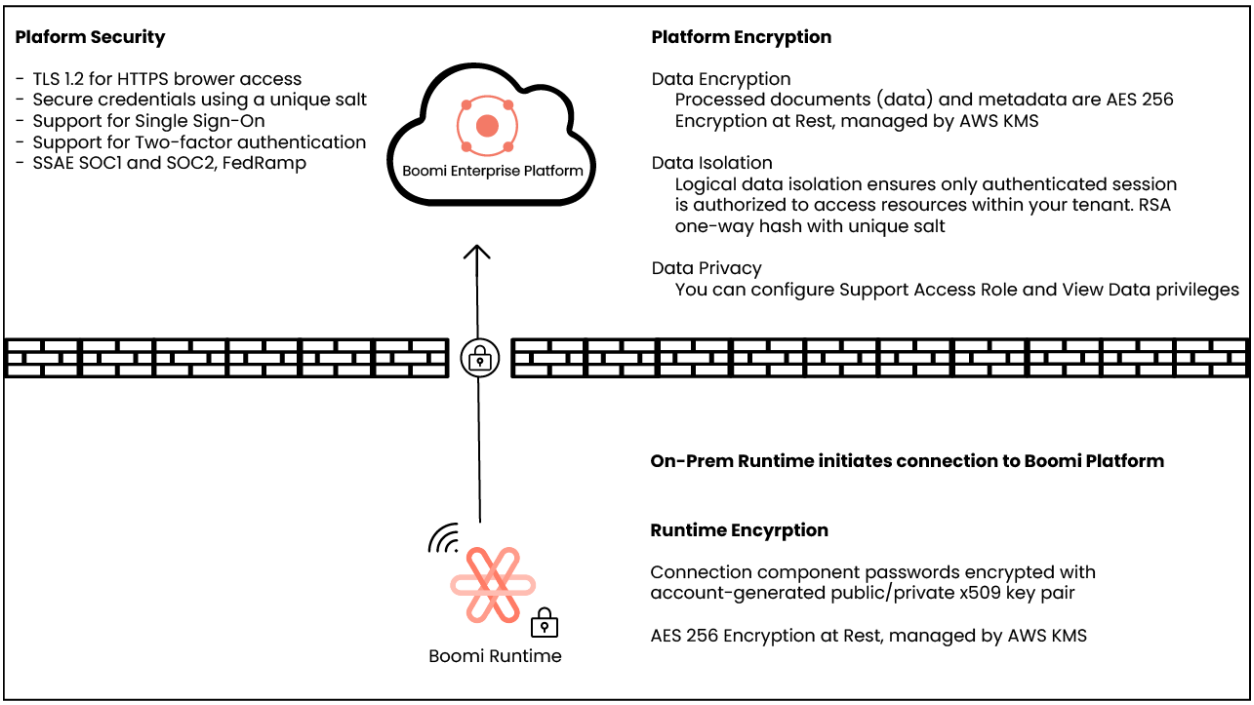

Diagram 3 - Boomi Platform - Encryption Architecture

Boomi and Subprocessors

Personal data that is processed via the Boomi Services, may be further processed by Boomi, or our subprocessors. Boomi's subprocessors list is available at www.boomi.com/legal/sub-processors. In line with the General Authorization principle set out in the Standard Contractual Clauses, customers have the option to subscribe for updates to the subprocessors list.

Data processing by Boomi and the transfer of Customer Personal Data for further processing by our subprocessors is subject to the terms of customer specific contracts with Boomi, and any agreed upon Data Processing Agreement (DPA). As set out in our Service Agreements, Boomi (i) takes responsibility for the actions of our subprocessors; and (ii) has written agreements with each subprocessor that contain data protection obligations, obligations that are materially similar to those contained in our Customer Agreements.

Boomi utilizes subprocessors, to provide third-party infrastructure, and host providers, including AWS and Azure, to deliver Boomi Services to our customers.

Managed Cloud Services

Overview

Managed Cloud Services (MCS) provides dedicated infrastructure hosting services for various Boomi and third-party ancillary products. These services are just as configurable, scalable and secure as a self-hosted on-premises solution, but they retain the benefits of a managed zero infrastructure footprint service.

High Level Architecture

MCS deploys its infrastructure within a dedicated, customer specific, virtual network based on the customer provided IP (CIDR) ranges. This allows customers to treat MCS as a natural extension of their own private network, allowing connectivity to internal/private endpoints, such as databases and other backend systems otherwise not reachable over the public internet. Private network connectivity can be established with on-premises networks via site-to-site VPN (IPSec) technology and/or via cloud peering solutions, if the MCS is co-located with an existing customer cloud network. These options are outlined in the diagram below.

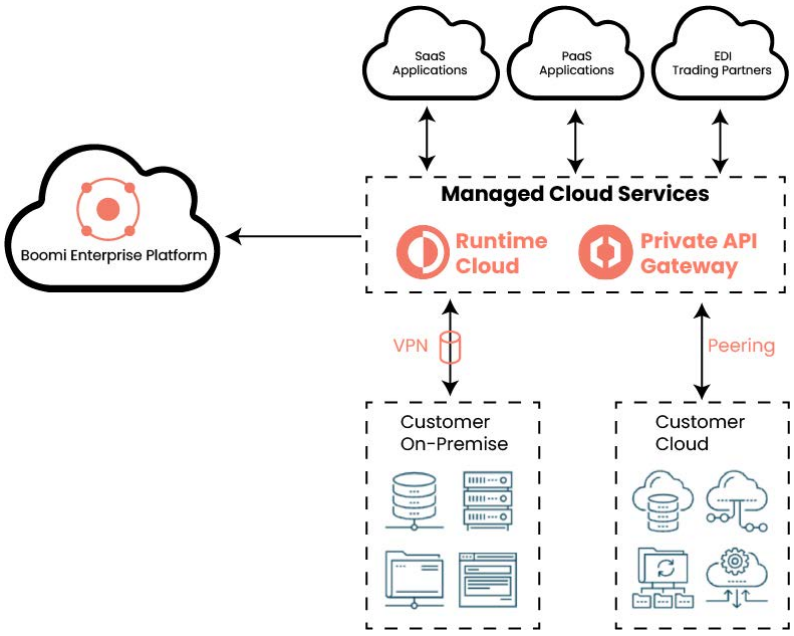

Diagram 4 – Boomi MCS Architecture

Data Flows

MCS provides dedicated cloud hosting solutions which allows the data flows to operate like a customer-hosted Boomi deployment. Boomi's products, data processes and storage, whether hosted by the customer, or by Boomi MCS, behave identically.

The diagram above represents a typical MCS deployment connecting various public and private (both on-premises and/or cloud) endpoints and highlights in red where data exchanges may occur.

By design, data security is a shared responsibility between the service provider hosting the infrastructure (here MCS) and the application-level users (customers, third-party providers, GSI, etc.). Therefore, both parties must acknowledge that security considerations and encryption capabilities are linked not only to how the products are hosted, but also to how they are configured and used.

Use-Cases

More details on possible use-cases are in the table below:

Type	Examples	Description
Public Endpoints	SaaS, Cloud, PaaS, B2B, etc.	Public endpoints are typically accessed over the public internet and secured in transit via encryption at the communication protocol level (TLS, SSH, etc.). Optionally, GPG payload encryption can be configured for heightened security. It is the responsibility of the customer, or any third-party service provider acting on their behalf, to develop integrations that leverage industry standard security protocols to secure the data flows.
Private Endpoints	Cloud, on-premises backend systems, databases, etc.	Private endpoints are accessed via a private network connection, such as VPN or direct cloud network peering. Data in-transit security is achieved at the network level with optional additional encryption at the communication protocol or payload levels (depending on customer requirements).
Boomi Enterprise Platform Endpoints	Platform API endpoints	Boomi Enterprise Platform endpoints are accessed over the public internet and secured via TLS. All communications are initiated by the Boomi runtimes (hosted in MCS) and by default, only Boomi Enterprise Platform Metadata is sent to

		Boomi Enterprise Platform. Under certain explicit opt-in conditions, payload data can be sent to Boomi Enterprise Platform, such as the: • View/Download Data feature – if enabled • Tracked Fields key value pairs – if configured • Boomi Assure test cases, and • Boomi Enterprise Platform Event notifications and/or exceptions – if configured • Boomi AI These product mechanics apply regardless of the hosting option (Public vs. MCS vs. customer hosted).
Data at-rest	Data archives and logs	Data at-rest is by default, retained on the runtime's filesystem for 30 days. Data, log and other asset retention are configurable in a variety of ways and can be customized to suit individual customer requirements, including the option to immediately purge the data. Any persisted data is encrypted at-rest, and any direct infrastructure access is highly secured and restricted.

Boomi Integration

Overview

Boomi Integration enables customers to use Boomi to move data between various applications, databases, and data sources. The customer, not Boomi, is responsible for where data is extracted from and sent and for designing integration processes that handle data appropriately. The following sections describe the data flows associated with the Boomi Integration Services and do not include considerations as to where customer specific destination applications are located.

Integration Deployment and Runtimes

Depending on the customers preference, the runtime can be deployed to Boomi's Public Cloud Service (PCS), Boomi's Dedicated Cloud Service (DCS), Boomi's Managed Cloud Service (MCS),

or to the customers' on-premise infrastructure whether the customers' own datacenter or a third-party datacenter.

For customers and partners using Boomi's Hosted Cloud Options, the Runtime(s) are hosted and managed by Boomi in Boomi's cloud (AWS). By design and default, no data from the Boomi cloud passes through the Boomi Enterprise Platform (see "View Data" section below).

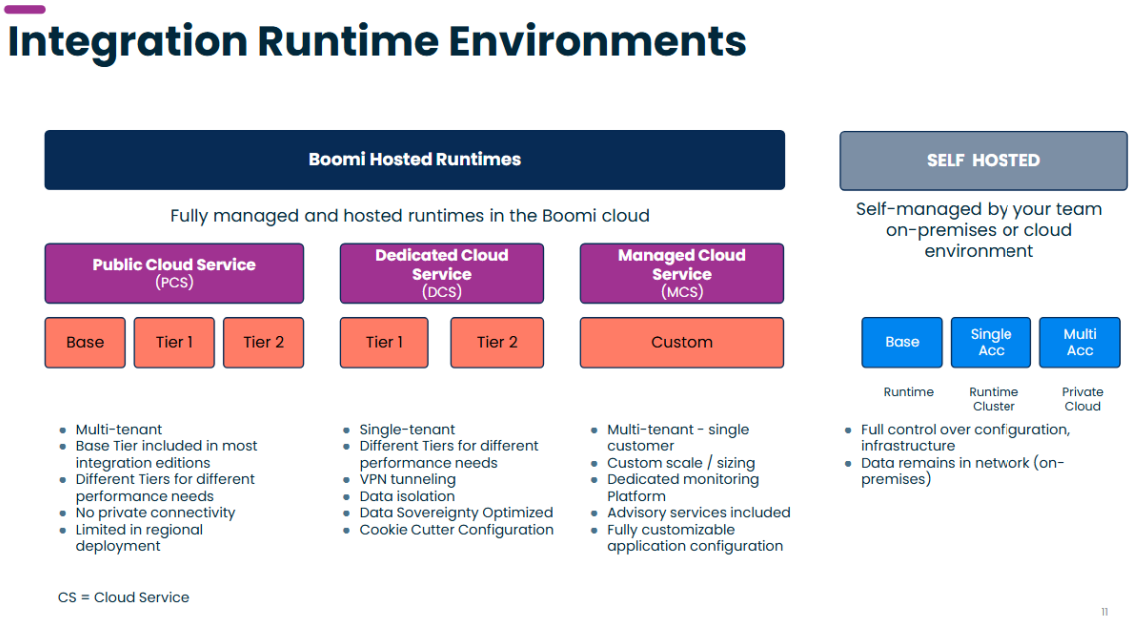

Diagram 5 – Boomi Runtime Deployment Options

The above diagram details the different deployment scenarios for the Boomi runtimes. In the diagram, "Boomi-Hosted" describes a runtime cloud that is hosted and managed by Boomi within a datacenter in North America, EMEA, or APJ.

Data Storage and Execution Behavior

As outlined above, Boomi supports multiple runtime hosting options, including customer-hosted deployments and Boomi-hosted environments. The main difference between these options lies in where integration execution data is stored.

- **Customer-hosted runtimes** store all execution artifacts–such as processed data and logs–locally within the customer's own infrastructure. This data is never sent to or stored in Boomi's cloud or systems.

- **Boomi-hosted runtimes** store execution artifacts within Boomi's secure, cloud-based infrastructure. This data is protected using disk-level encryption and is accessible only to authorized users.

Boomi's MCS offerings (and dedicated cloud services) also support optional VPC or VPN connectivity allowing secure communication with your local applications and data sources.

Regardless of deployment type, all data processing occurs entirely within the runtime, which connects directly to your endpoints. The Boomi platform never processes or transforms document data.

Data Visibility and Logging

Boomi collects and displays limited metadata from your integration processes for operational and troubleshooting purposes. This includes:

- **Execution Metadata**, such as process duration, success/failure status, number and size of documents process, and error messages. Actual document content is never collected or stored by the Boomi platform. To protect sensitive data, avoid including personal or confidential information in customer error messages.
- **Platform Events** indicating when a process starts, stops, or encounters an error
- **Runtime Details**, such as online/offline status, startup configurations, and infrastructure information (e.g., operating system, Java version).
- **Tracking Fields**, which can be configured to monitor specific data points in connector steps. As with error messages, customers should avoid logging sensitive data in these fields.

Runtime Logs and Access

Boomi offers several types of logs to help monitor runtime operations:

- **Runtime** logs can be viewed or downloaded via the platform or UI or API. These logs are transmitted only temporarily to the browser or API client and are not stored in the Boomi platform.
- **Container** logs provide insight into the runtime engine's behavior and can assist runtime administrators in system monitoring.

- **Shared HTTP Server** logs record all inbound HTTP requests to the runtime's shared web server. These are especially useful for debugging service calls that do not result in full execution flows.

Private Cloud Runtime Solution

In the Private Cloud architecture, Boomi hosts the customer runtimes on our single-tenant cloud, eliminating the need for a customer managed infrastructure.

Boomi's Private Cloud Runtime Solution supports the following connectivity's :

- Cloud to Cloud,
- Cloud to on-premises, and
- On-premises to on-premises.

Boomi's On-Premises Runtime Solution

The Boomi On-Premises Runtime Solution provides split architecture of the Boomi Enterprise Platform and Boomi Runtime allowing customers the option to decide the separate placements of runtimes for security, performance, or data sovereignty purposes, for example.

In this hybrid architecture the Boomi Runtime is installed on the customers' on-premises infrastructure within the four walls of their datacenter.

EDI

Overview

Boomi's EDI capabilities are an extension from its core Integration service offering. Customers may use Boomi EDI to send messages between various EDI trading partners via any number of industry standard communication protocols such as AS2, Disk, HTTP, FTP/SFTP, OFTP2, and MLLP (available on Boomi's Documentation at help.boomi.com). The Customer, not Boomi, is responsible for determining where its data is sent and for designing integration processes that handle data appropriately.

Data Integration

Overview

Boomi Data Integration provides a simple way for customers to migrate data from their applications, databases, files and events to their preferred data warehouse. Data Integration uses the TLS 1.2+ Protocol to encrypt data in transit and at rest, data is encrypted and stored in AWS' EFS storage service before being transmitted to a target. Boomi Data Integration offers data ingestion, data transformation, ETL, reverse ETL, data orchestration, data ops management, and CDC replication solutions.

Data Types

Boomi Data Integration uses your various metadata to provide the services and process Processed Data by transferring that data from source to target. Boomi also collects your Design Time and Runtime Configuration Data for the purpose of monitoring usage, error resolution, support, and Activity Logs.

Subprocessors

In addition to as described above, Boomi Data Integration uses two subprocessors for all customers as set forth below.

Subprocessors	Entity Country	Purpose
Amazon Web Services Inc.	Global, United States, Ireland	Hosting services
Google, Inc.	United States	BigQuery Data warehouse

Additionally, Boomi Data Integration may use Pipeline Data Subprocessors for customers who employ non-core infrastructure Data Subprocessors to support particular product features, such as specific destination partners.

Subprocessors	Entity Country	Purpose
Google Inc.	Global	Google Cloud Supplier Data Destination
Snowflake Computing, Inc.	United States	Supplier Data Destination
Microsoft, Inc.	United States	Azure Supplier Data Destination
Amazon, Inc.	Global, United States, Ireland	AWS Supplier Data Destination

Architecture / Data Flows

Boomi Data Integration can be hosted in the United States and Europe and uses AWS as the cloud provider.

Region	**Cloud Region**
US	us-east-2 (Ohio)– 3 AZ
EU	eu-west-1 (Dublin)– 3 AZ
IL	il-central-1 (Israel) - 3 AZ
AU	ap-southeast-2 (Sydney) - 3 AZ

Below is a diagram of the data flow using Boomi Data Integration.

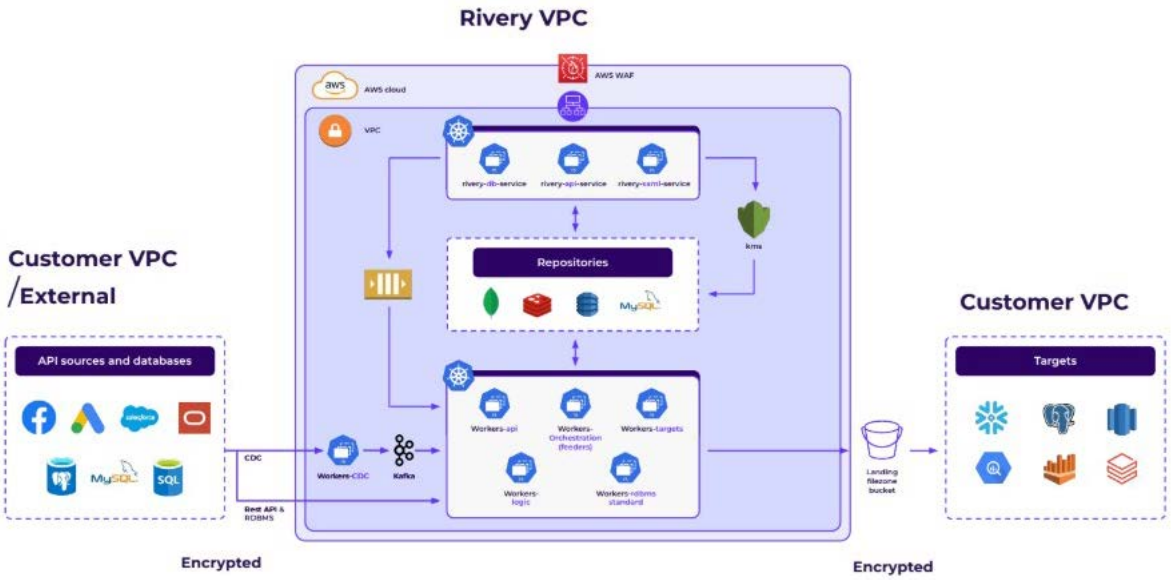

Diagram 6 – Data Integration Architecture

Advanced Connectivity

Boomi Data Integration also offers various advanced connectivity options such as VPN Tunnels, PrivateLink (AWS, GCP, Azure), and Reverse SSH. When using a VPN Tunnel, a dedicated VPC is provided with no connection to the internet. The AWS Site to Site VPN provides a secure connection between this dedicated VPC to the Customer VPN.

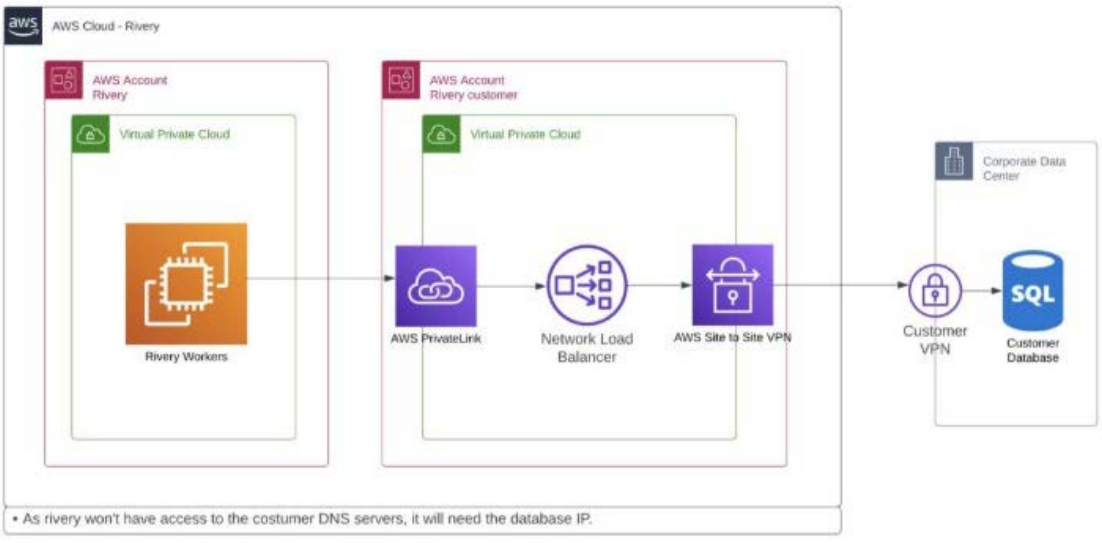

Diagram 7 – Data Integration Advanced Connectivity

Reverse SSH Tunnels work similarly to SSH Tunnels except that the SSH Tunnel is not run on the customer side, but on the Boomi side. Boomi will configure a dedicated SSH Tunnel Server with SSH keys provided by the customer. The customer will then have to establish a connection with the SSH jump server. With this option, the SSH Server is managed by Boomi and the connection is initiated by the Client Network.

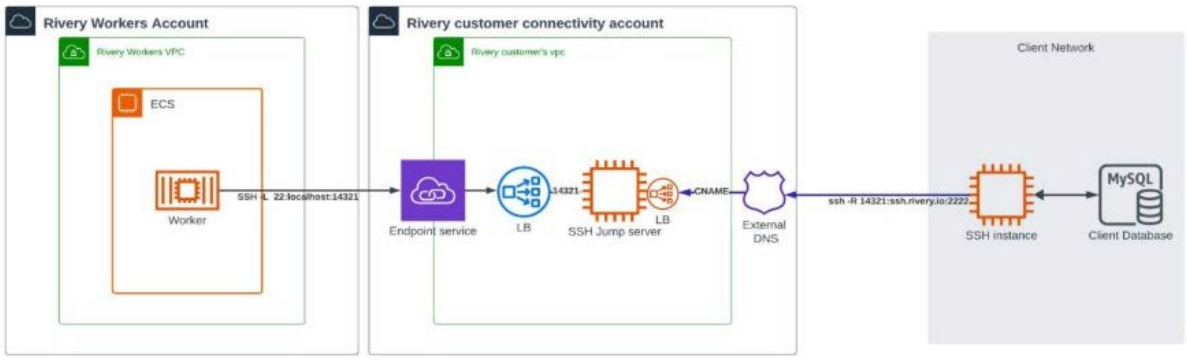

Diagram 8 – Data Integration Reverse SSH Tunnels

Boomi Data Integration Agents

Boomi Data Integration has two separate agents designed to help develop integrations between source and target destinations, and to ask questions about the operability of Boomi Data Integration,

Data Connector Agent

The Data Connector Agent consumes data from externally sourced REST API documentation to understand API endpoints, authentication methods and data structures. The Agent provides an output consisting of YAML configuration files, interface parameters, ETL pipeline configurations, and debug and validation data. This data is encrypted to ensure that no sensitive information is passing through the agent ensuring that only metadata configuration is processed by the agent.

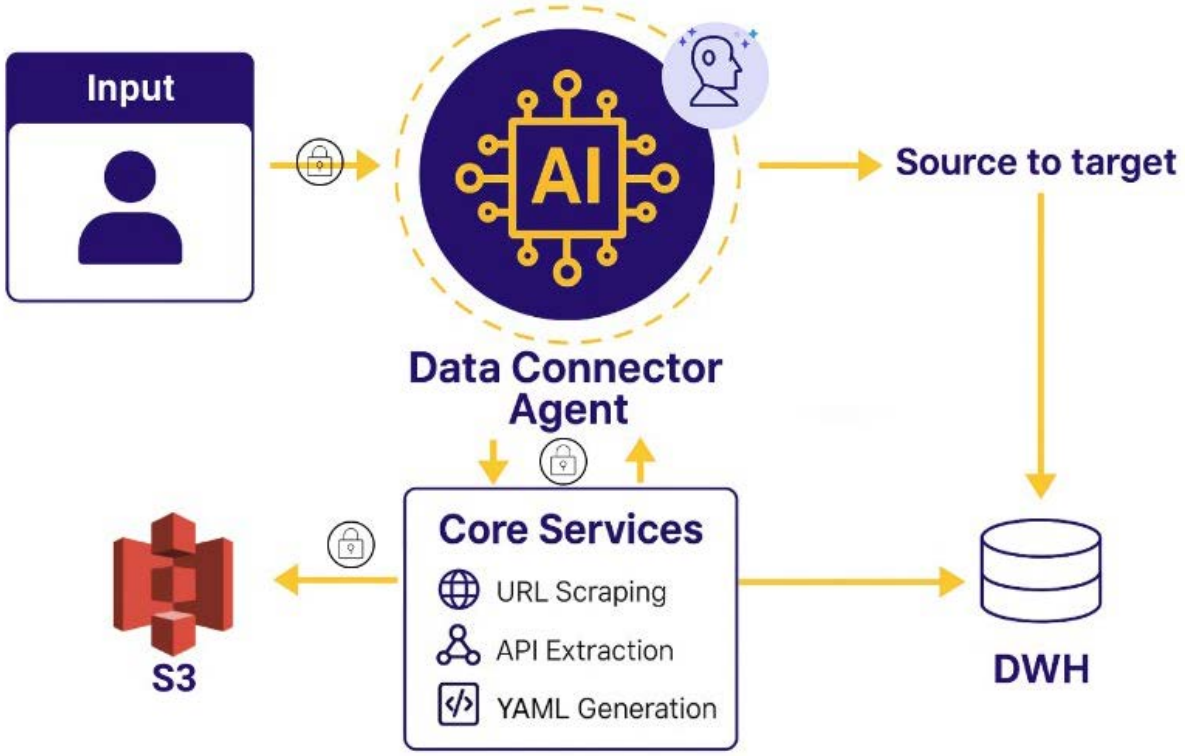

Diagram 9 – Data Connector Agent Architecture

Data Integration Ask AI Agent

The Data Integration Ask AI Agent is an intelligent assistant embedded within the Data Integration platform, designed to deliver instant, accurate responses to technical questions by leveraging Boomi's extensive knowledge base including product documentation, API references, and user community insights. Ask AI provides quick, relevant answers, helping streamline data integration tasks and improve workflow efficiency. Data Integration Ask AI draws exclusively from publicly available resources to ensure accuracy and data security.

Boomi AI

Overview

Boomi AI currently consists of Boomi AI Agents and Boomi Agentstudio. Once an account administrator approves the use of Boomi AI for an account, users can create, govern, and interact with AI Agents through Boomi Agentstudio.

Boomi AI Foundational Large Language Model Use

Customer data is not used to train or fine-tune any Boomi models or foundational large language models used by Boomi AI. Third-party providers of the foundational LLMs will not share your data and Boomi will only share your data with the Third-party providers of the foundational LLMs solely for the purpose of providing the services.

Boomi AI Data Boundaries

Agent data, encompassing the knowledge bases and data stores, as well as the foundational LLM and ML models, are deployed within data centers in North America. Importantly, all data, including a user's conversational interactions, remains exclusively within these regional boundaries and is not replicated beyond them. All data is encrypted, both at rest and in transit. For Agents created with Boomi Agent Designer (discussed below), sensitive data is additionally encrypted with a customer account-specific encryption key.

Boomi AI Agents (Platform Agents)

Boomi AI Agent Features

Boomi Platform Agents allow customers to perform certain actions within the Boomi Enterprise Platform using natural language. Boomi's Agent Garden, accessed through Agentstudio, includes the following native Boomi Platform Agents.

1. **Boomi GPT** - conversational user interface that collaborates and calls on other Boomi AI agents to take actions.
2. **Boomi DesignGen** - autonomously designs integration processes based on 300M+ integration patterns. Users also have the ability to directly edit processes designed by Boomi DesignGen using natural language.
3. **Boomi Pathfinder** - provides next best steps guidance, when building integration processes - with automated data mapping, building blocks, and more.
4. **Boomi DataDetective** - classifies data fields, and tracks where personal or sensitive data is moved geographically.
5. **Boomi Scribe** - automatically creates documentation for your integrations (including those built-by-AI).
6. **Boomi Answers** - offers prescriptive guidance and delivers answers about the Boomi Enterprise Platform and its functionality grounded by relevant knowledge-bases

7. **Boomi HubGen** - streamlines data model creation to accelerate data synchronization across your enterprise. HubGen generates models based on the type of domain desired and the sources involved in data synchronization.
8. **Resolve Agent** - autonomously troubleshoot integration process failures, to enhance operational efficiency with curated solutions and capture error details to reduce future disruptions.
9. **API Design Agent** - autonomously generate compliant and comprehensive OpenAPI specifications, to rapidly design and edit APIs tailored for your business and technical needs.
10. **API Documentation Agent** - autonomously generate business and technical documentation from API definitions, to accelerate time-to-market and increase adoption.
11. **Integration Advisor Agent -** offers a detailed review of your existing integrations and identifies gaps and improvements that can be made to increase the efficiency of your processes.

Boomi Platform Agent Architecture

The Boomi AI native agents architecture comprises of three primary components:

1. **AI Agents** - are autonomous or semi-autonomous pieces of software that can understand natural language and take actions to accomplish a goal.
2. **Models** - Boomi AI Agents use two types of AI models: Foundational Large Language Models (LLM) and traditional machine learning (ML) models. The LLMs are used by the Platform Agents for planning, reasoning, embeddings generation and content generation. The traditional ML models are primarily used for prediction, intent classification, and named entity recognition.
3. **Knowledge Base/Data Stores** - Boomi Platform Agents use multiple knowledge bases and data stores for content retrieval during certain agent executions. This data is used as part of a retrieval-augmented generation (RAG) pipeline or returned as part of the agent's output.

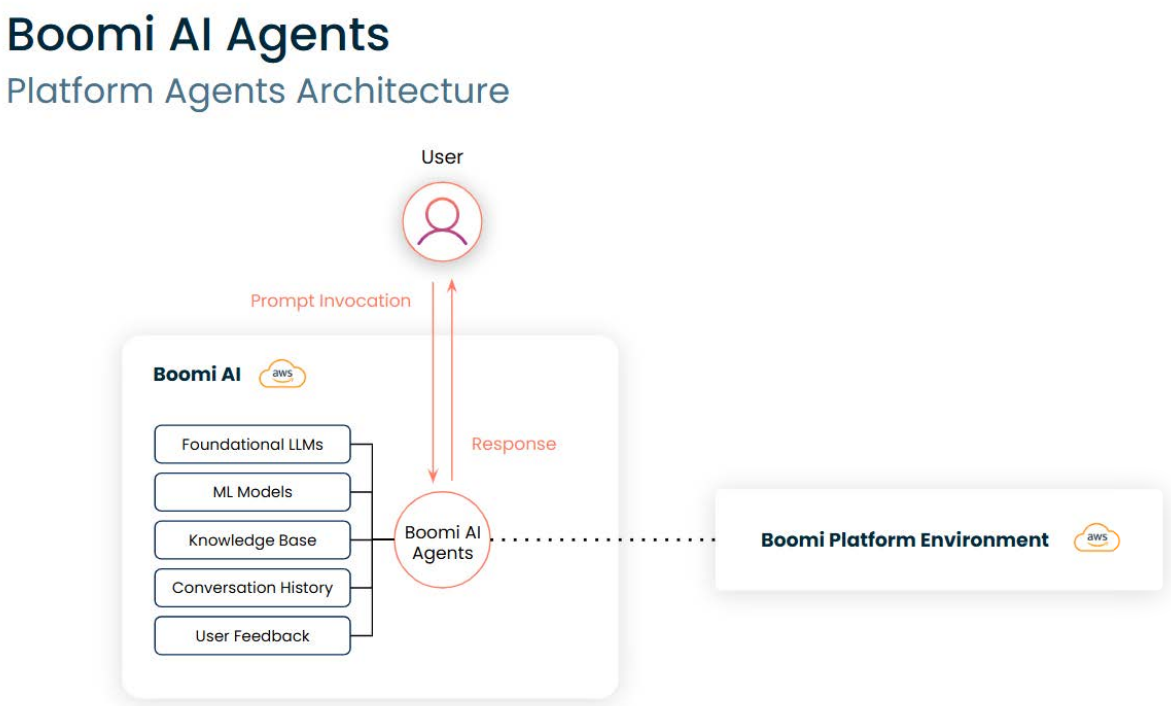

Diagram 10 – Platform Agent Architecture

Boomi Platform Agent Use of Collected Data

Boomi Platform Agents use de-identified metadata (i.e. Design Time Configuration Metadata) in aggregated form to support improvement of Boomi's intelligence features as outlined at our data collection process. Customers can opt out of this process by following the process outlined here.

Your prompts/conversation history are not processed as part of the data collection process, and are neither analyzed or used to improve Boomi's AI features. Even when you opt-out to usage of data by Boomi, you can still use the Platform Agents[1] and Agentstudio and Boomi will process and store the data as outlined below.

Data flows within Boomi Platform Agents

As the primary interaction between a user and Boomi AI is conversational and the data flows between the components depends on both the user's intent and the AI agent with which they are interacting.

[1] Excluding Boomi Data Detective

Item	Name	Description
1	Conversation History	Conversation history data is a structured record of interactions between a user and an AI Agent. This data may include timestamps, user input, agent responses, and potentially metadata such as confidence scores, actions taken, and context information relevant to the conversation. This data is encrypted in transit and at rest.
2	User Feedback	User feedback of an AI Agent interaction is user provided ratings, such as a "thumbs up" or "thumbs down," along with an optional text comment explaining their satisfaction or dissatisfaction with their interaction with the Agent.

Design Time Configuration Data is used or generated by several of the Boomi AI Agents, for example:

- **Scribe** - Retrieves Design Time Configuration Data from the Boomi Enterprise platform in order to generate Integration process documentation.
- **DesignGen** - AI generated Design Time Configuration Data of an Integration process is created and presented to the user. Upon user approval of the generated configuration, this data is persisted in the Boomi Enterprise Platform just as would be with a manually-created integration process.
- **HubGen** - AI generated Design Time Configuration Data of DataHub models is created and presented to the user. Upon user approval of the generated configuration, this data is persisted in the Boomi Enterprise Platform just as would be with a manually-created DataHub model.
- **DataDetective** - Uses Design Time Configuration Data from the Boomi Enterprise Platform to identify fields containing sensitive data such as PII and determine where this data moves geographically.
- **Integration Advisor**- Retrieves Design Time Configuration Data from the Boomi Enterprise platform in order to understand the process XML and provide recommendations for improvement.

Agentstudio

Agentstudio Features

Boomi Agentstudio is comprised of the following:

1. **Agent Designer -** Design component that allows the creation of custom AI agents from scratch, with AI assistance, or with pre-built templates. Customers and Partners can power and ground agents with trusted enterprise data and knowledge using tools connected to the Boomi Enterprise Platform. Enforce secure and ethical agent behaviors with guardrails, and refine performance through robust testing**.**
2. **Agent Garden -** Manage agents and their tools across their lifecycle including building, testing, and deployment within one unified space. Customers and Partners can interact with AI agents using natural language.
3. **Agent Control Tower -** Manage, monitor, and govern AI agents from Boomi and third-parties across your organization with centralized registry. Customers and Partners can monitor performance and detect anomalies to reduce security and compliance risks.

Agentstudio Data Types within Boomi Agentstudio

Item	Name	Description
1	Agent Specification	The definition of an AI Agent developed by the Boomi customer using the Agent Designer. This data includes items such as an agent's goal, personality, tasks, instructions, guardrails, tools and conversation starters.
2	Tool Specification	The definition of tools which can be used by agents in the Agent Garden. The configuration data depends on the tool type.
3	Tool Outputs	Tool Outputs are normally processed by the Boomi Platform Environment for agent execution, but not stored. If the “data passthrough” configuration is set on the Tool, then the tool output only passes through the Boomi Platform.

4	Agent Session	The state of a conversational session between a user and an agent in the Agent Garden. This data includes but is not limited to prompts sent via the chat or via agent step, agent responses, conversation history summary and guardrail activations.
5	Agent Provider and Agent Metadata	Agent metadata that describes the configuration of agents. This includes status, trust level, tags, tools, tasks and guardrails.
6	Agent Usage Metrics	Any agent usage metrics reported, by an agent provider, to the Agent Control Tower. This data includes, but not limited to, time-to-first-token, token usage, client errors, server errors, guardrail enforcement and execution time. Metrics that are available vary between providers.

Agentstudio Architecture

The Boomi Agentstudio platform allows interaction between an agent built within the Agent Designer, through a chat interface or via an Agent Step within a deployed integration process.

Data Flow of User Invocation to Agentstudio via Chat

This method, depicted in the Agent Chat Data Flow diagram, involves a direct conversational interaction between a user and an agent. The user sends a prompt, and the agent, hosted within the Boomi Platform Environment, processes the request. The agent's response, along with the full chat history, is maintained and encrypted in the Agent Session Database. This interaction is conversational, and the session information (e.g. chat history) is stored indefinitely unless the user deletes it. Alternatively, tool outputs are not stored.

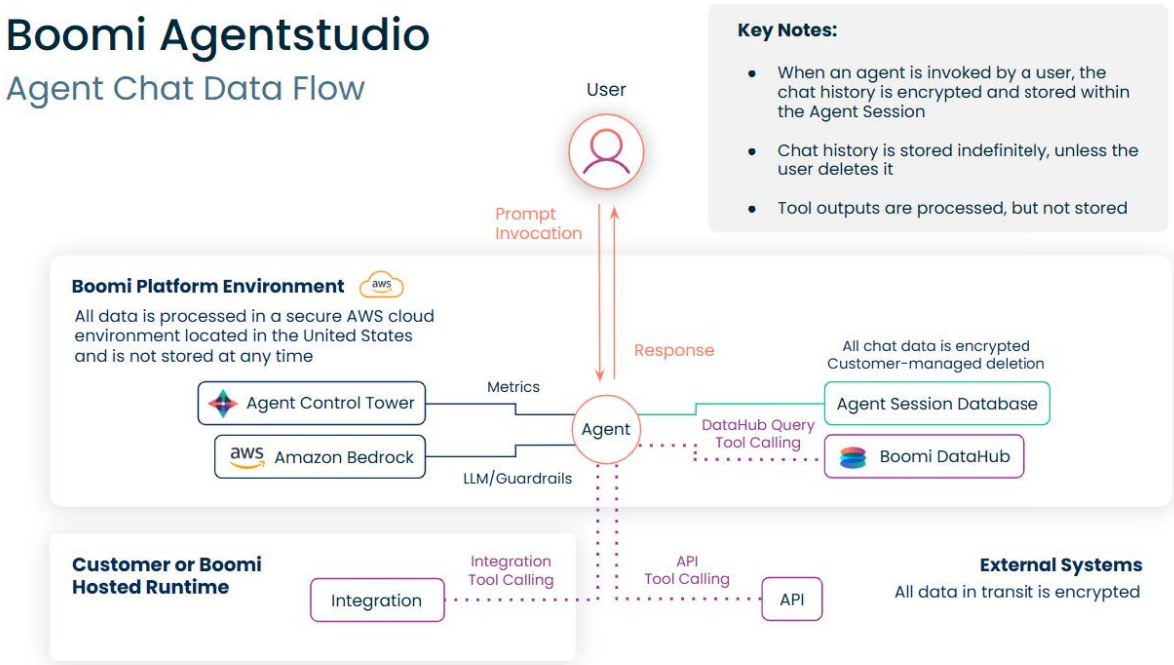

Diagram 11 – Agentstudio Agent Chat Architecture

Data Flow of Invocation from an Agent Step in a Deployed Integration

This method, shown in the Agent Step Data Flow diagram, integrates an agent's functionality directly into an existing Boomi integration process. A deployed integration, running on a Customer or Boomi Hosted Runtime, uses an Agent Step to send a prompt invocation to the agent. The agent processes this request and returns a response, which is then used to continue the integration process. In this data flow, the prompt and response are processed by the agent, but the conversation history is not stored since it's an automated, non-conversational interaction. This is distinct from the chat flow, where a user-centric conversation is the primary purpose.

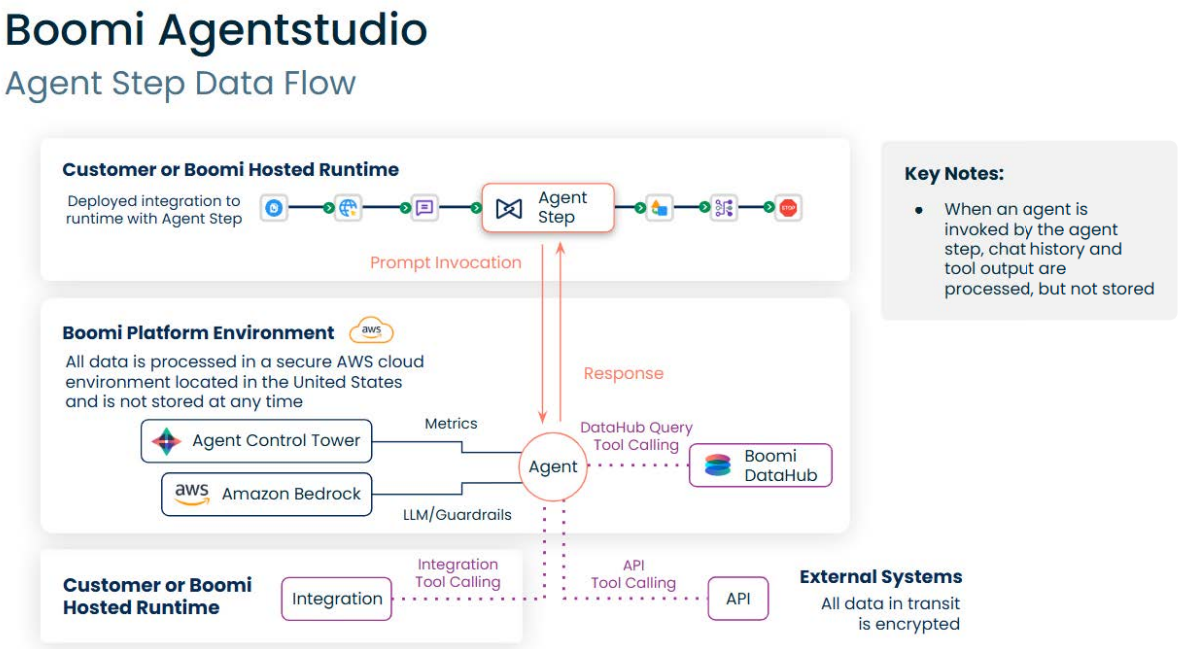

Diagram 12 – Agentstudio Agent Step Architecture

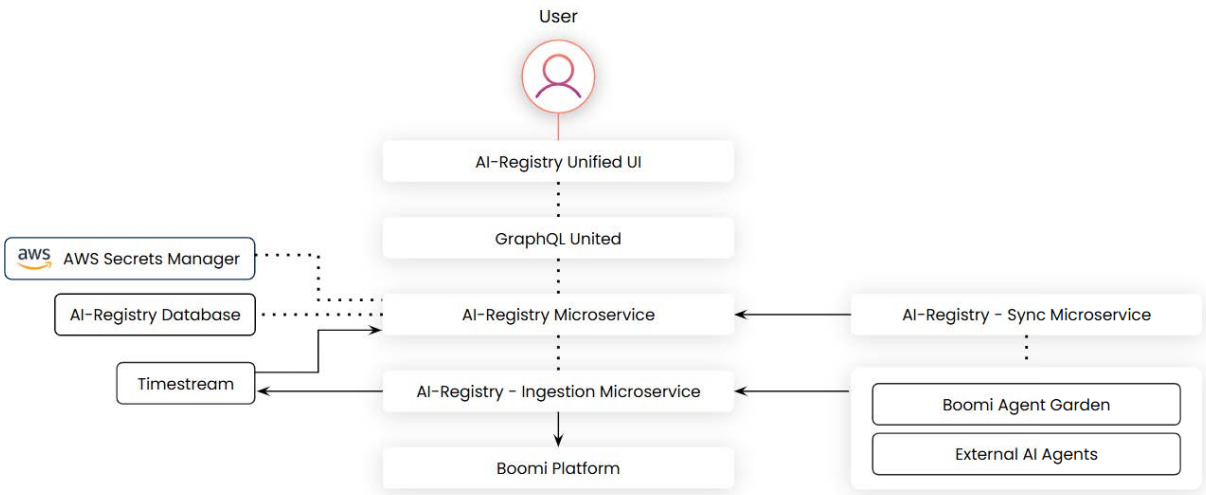

Diagram 13 – Agentsstudio Control Tower Architecture

Boomi API Management

Boomi API Control Plane

Overview

The API Control Plane is an essential component of Boomi's API Management capabilities. It provides a centralized framework for managing and governing APIs within an organization. It uses a federated approach, providing centralized governance across your API landscape while leveraging existing investments. This ensures comprehensive oversight without disrupting current infrastructure. To do so, the API Control Plane connects to multiple API gateways. This includes, but is not limited to the Boomi API Gateway and Boomi Cloud API Management. The API Gateway is a specialized Boomi runtime dedicated to access control, security, and policy enforcement for APIs and is only available if the Runtime is deployed on-premise or on Boomi DCS or MCS. The Gateway can be deployed by the customer alongside the runtimes hosting their APIs.

Control Plane Architecture

The API Control Plane consists of the following components:

- the Control Plane backend
- the Administration Portal
- the Developer Portal
- the Control Plane agents

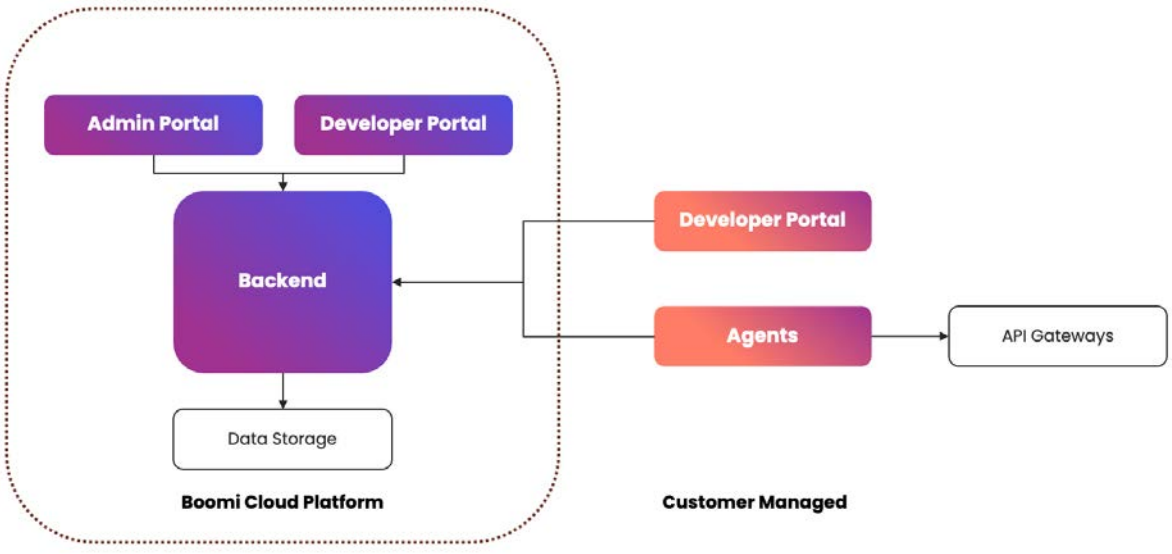

Diagram 14 – APIM Control Plane Architecture

The **Control Plane** backend (hosted inside of the Boomi Enterprise Platform - currently only available in the US) provides the functionality for both the admin and developer portals. API Control Plane does not interfere with the actual traffic of the APIs and is unaware of all data that is received or transmitted by the gateways.

The **Administration Portal** is the interface that you see when you log into your API Control Plane. It is used to manage and govern the APIs that are discovered on your gateways and is part of the Boomi Enterprise Platform.

The **Developer Portal** is where consumers of your API can discover your APIs, read the documentation, and get access to your APIs. Developer Portals are hosted by Boomi as part of the Boomi Enterprise Platform but depending on the use case, can also be self-hosted in your private cloud or on premises.

Control Plane agents facilitate the communication between your gateways and the API Control Plane. The agents are either hosted by Boomi (for Boomi API Gateway and Boomi Cloud API Management) or by you (for all other gateways). The agent is the only entity that needs the credentials to access your gateways. The credentials are injected into the agent and can be stored in any secure vault you may be using. The API Control Plane backend does not have knowledge of these credentials. They are not stored or transmitted to our cloud platform. The connection between the agent and the backend is initiated by the agent, thus no inbound firewall rules or site-to-site VPNs are needed for operation. The following figure illustrates an example data flow.

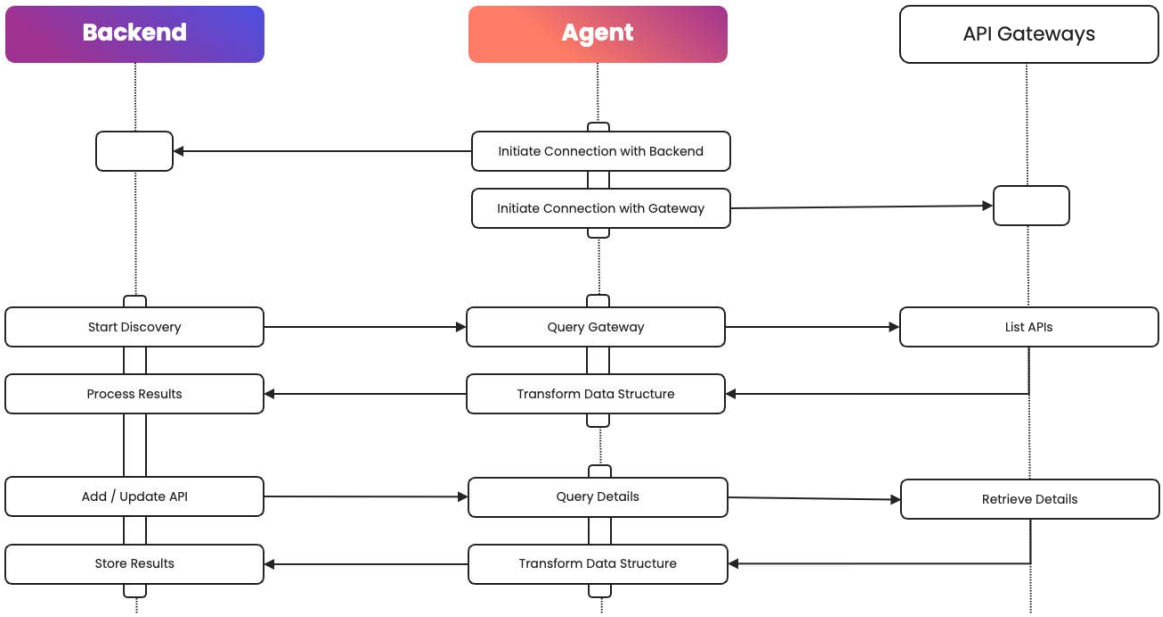

Diagram 15 – APIM Control Plane Agents

The following types of data apply specifically to the API Control Plane

Name	Description
API subscriptions and API keys	API subscriptions as well as keys are also stored inside of the Boomi Cloud. API keys are not considered to be sensitive information. In case the API requires API secrets, those are NOT stored inside of the Boomi Cloud. They are just transferred once in order to visualise them to the user as part of the admin and developer portals.
API payloads	The payloads used in calls to non-Boomi API gateways are not stored as part of the Boomi API Control Plane, meaning any data consumers send to the APIs or returned from the API is not visible to the Control Plane and not stored. See the sections on Boomi API Cloud Management and Boomi API Gateway for a description of the respective data flows.

Boomi Cloud API Management

Overview

Boomi Cloud API Management delivers the ability to secure, manage, productize and provide access to APIs at enterprise scale. The solution was designed at conception to be cloud-native, elastic and highly available. This means that whether customers elect to leverage it in a fully Boomi-hosted (multi-tenant SaaS) manner, or by deploying traffic management capabilities on-premises, they have an offering that can scale infinitely and meet enterprise-grade availability to support mission critical business requirements.

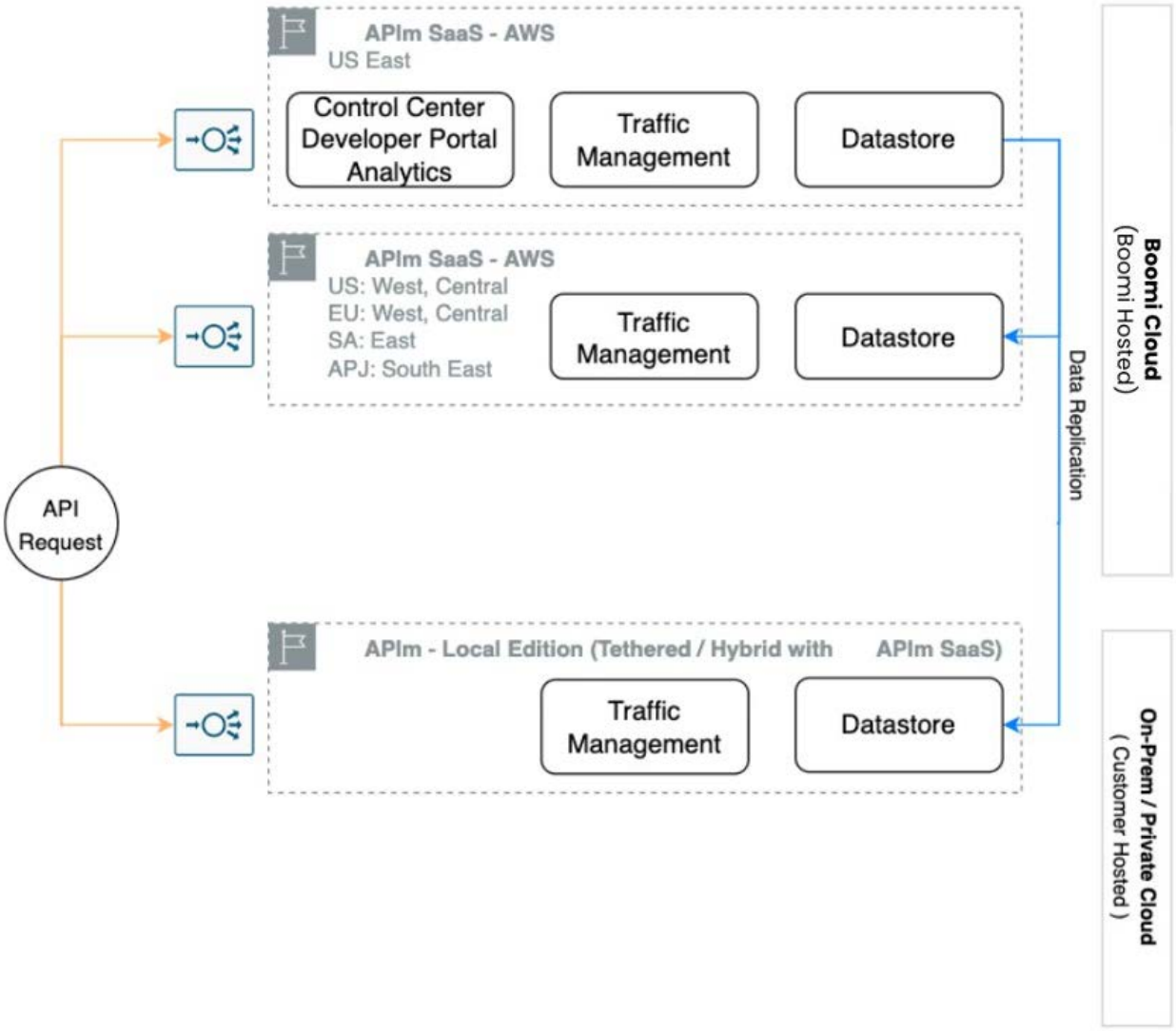

Diagram 16 – API Management Architecture

Key Components

Cloud API Management consists of four functional components that make up the solution set.

Developer Portal
The Developer Portal acts as the API Discovery, interaction and self-service onboarding area for API Consumers. Customers can customize the look and feel, along with the type of content that is published based on the target audience of API Consumers. This includes, for example, interactive and long-form documentation and product marketing assets.

Control Center
The Control Center is a web based design time interface leveraged by API Providers (Customers) to define and manage API policies, content within the Developer Portal, security and user access-controls, and access reporting and business value dashboards.

Traffic Management
Traffic Management is the key component in processing inbound and outbound API transactions from API Consumers. While functionally serving as an API Gateway, the component also includes other critical roles including, but not limited to, replicating API quota, throttle counters, and propagating change management updates made via the Control Center, across the implementation footprint.

This capability is available both within the multi-tenant Boomi hosted SaaS solution, and on-premises via Boomi's Cloud API Management Local Edition (on-premises) offering.

Datastore
The Datastore is an aggregation point for all API Policy configuration, user management, reporting and analytics data, along with cached content (as applicable) that is distributed across the Implementation footprint.

The Datastore extends to customer' on-premises deployments, when leveraging Cloud API Management Local Edition clusters.

Cloud API Management Data Flow & Management

Cloud API Management API Consumer (Developer) User Registration

Flow 1 – API consumers registering with the Boomi-managed Developer Portal Identity Management solution operating within the Cloud API Management SaaS platform

- API consumer initiates a registration process on the Developer Portal and provides API consumer Registration details (First/Last Name, Email, Company, etc)

- API consumer data is captured in Datastore and is replicated across all APIm regions
- API consumer data is leveraged and referenced for use when creating, registering or using API Applications; specifically, when processing API Requests in order to appropriately monitor and track access controls and counting (e.g. limits or quotas)

Flow 2 – API Consumer registering with a customer-managed identity management solution

- API Consumer/Admin initiates a registration process on the Developer Portal and is redirected to the Customers' third-party identity provider (IdP) Provider for either account creation or sign-in
- API consumer either creates an account or signs-in via the third-party IdP
- Following successful account creation and/or sign-in, IdP completes Single Sign-On (SSO) handshake with APIm and returns:
    - Confirmation of successful login
    - Metadata for reference/stub account to be locally created in APIm for Application/Package/Key management
    - Key metadata details (First & Last Name, Username) can be serialized by the third-party IdP for further data protection, as needed.
- As the API Consumer continues to use APIm, the local stub/reference account serves as the point for Application and API Access details, with the third-party IdP continuing to serve as the source of truth and session management for the Developer & Control Center portals.

Flow 3 – API Consumer invited via Boomi Platform defined Identity Management Solution

- API Consumer is invited to join a Cloud API Management Developer Portal from within the User Settings section within a Customer's Boomi Enterprise Platform tenant
- Depending on how the Customer has set up their Boomi Enterprise Platform tenant, either Boomi's default identity management solution or the Customer's custom identity management solution (as configured in the Boomi Enterprise Platform) will be the source of truth for API consumer identity management
- The API Consumer, if not already registered as a user within the Boomi Enterprise Platform, receives steps via email to complete a registration process and provides details (First/Last Name, Email, Company, etc.)
- API consumer data is captured in the Cloud API Management Datastore and is replicated across all APIm regions

- API consumer data is leveraged and referenced for use when creating, registering or using API Applications; specifically, when processing API Requests in order to appropriately monitor and track access controls and counting (e.g. limits or quotas)

API Policy Definition and Management

Managed via the Control Center interface, or through Platform APIs, Customers can create and define new API policies and configurations that include critical details needed in order to receive, process and respond to API Requests made to the solution. These include URL domains, path addresses, and details around the access controls, and packages/products through which APIs can be available for consumption. This data is replicated across Boomi Cloud Hosted (SaaS) regions, and Local Edition clusters.

Application and Credentials Management

The features surrounding application generation, and key/credential generation provide API Consumers with the ability to onboard to API products and offerings, and to request access to them. When a request is approved, the API Consumer's application is issued a set of API key(s) and or secret(s) depending on the security mechanism defined. This data can in turn be used to authenticate directly, or to create tokens with broader user-context, prior to making requests to the solution. This data is replicated across Boomi Cloud Hosted (SaaS) regions, and Local Edition clusters.

API Transaction Handling

The features surrounding API request processing include validation of credentials and tokens for authentication, request path/policy mapping and routing, and the capturing and storage of API transaction metadata

Boomi Flow and Task Automation

Overview

Flow is a low code application, development, and hosting environment that enables customers to construct and execute browser delivered business applications. As a process orchestration

environment and application design tool, it is not a persistent data store and data should be stored in a persistent, managed system of record e.g., a database.

Flow Platform Architecture

Flow provides unique flexibility with split architecture of design time and runtime.
The design time API (which underpins the Flow design time UI and renders HTML pages into a browser) is hosted, managed, and maintained by Boomi on our Platform (AWS).
The runtime executes and delivers UI pages to the browser and can be hosted by Boomi, or the customer on their own infrastructure.

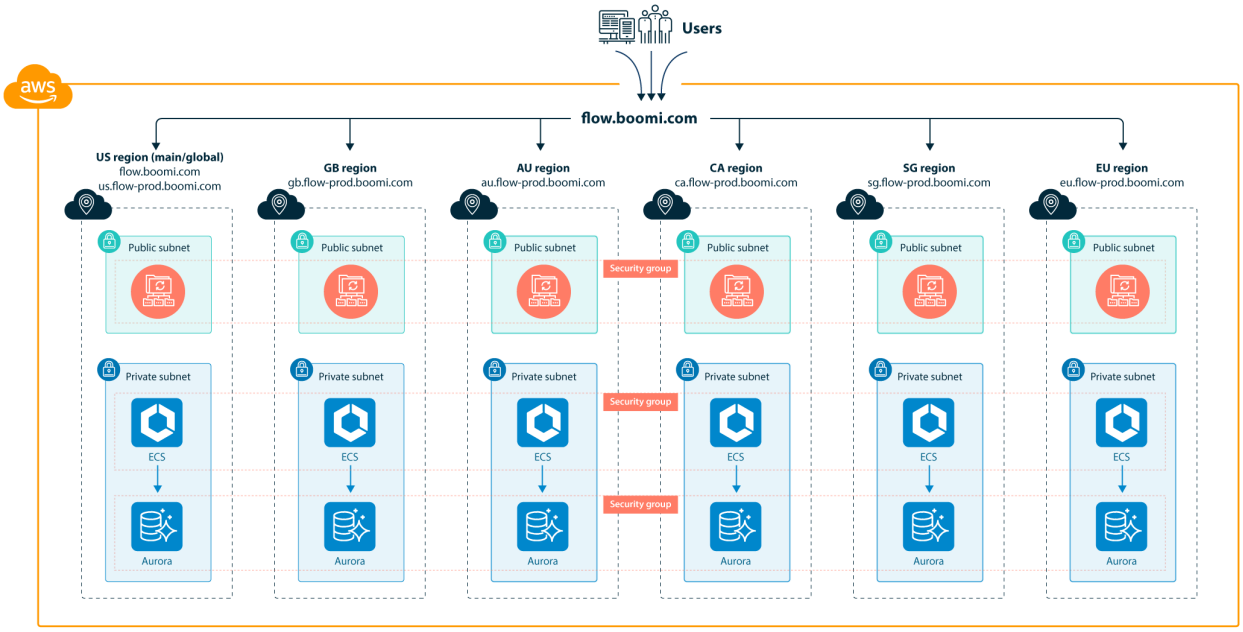

Diagram 17 – Boomi Flow Architecture

Data Flows within Boomi Flow

There is 1 distinct data element to Boomi Flow.

Name	Description
System of Record Data	Any data which should be persistent, whether as a source or target, is stored in an external system managed by the customer and exposed to Flow via an API.

	Flow uses the API to load data from the system of record as defined in the process, hold it in the state (from where the user can interact with it) and then update changes back to that system again (or some other target) as defined in the process. The process definition can also be used to purge the data from the state if required.

Runtime Configuration Metadata for Boomi Flow refers to data and settings which can be specified for an integration runtime or API Gateway. When a Flow executes, it generates a runtime data payload and process logs, which holds details of the execution, the route the process took through the predefined application definition with timings and the payload data. This data exists in the Flow internal database and is accessible via the design time UI from the "Dashboard" tool or via the API. This data is not persistent because it only exists for the length of time the process is running and a short configurable period afterwards. The data is automatically purged after a pre-defined (user selected) period and is then no longer accessible.

Data Boundaries

In Flow, both design and runtime data, is deployed exclusively into regional datacenters. Data is never replicated outside those regional boundaries.

Multi-Cloud

Flow can also be deployed into a multi-cloud environment. The runtime portion of the Platform can be deployed, as a docker image, into any cloud or local environment of the customer's choosing.

It is the responsibility of the customer hosting the underlying database to hold the process definition and state data. In this multi-cloud model, data is not replicated to or from the Flow regional datacenters. The data resides solely in the customer's infrastructure.

Flow Runtime Options

The following table details the different implementation scenarios for the Flow runtime.

Name	Description
Flow Platform	Boomi hosts and manages all design time and runtime data in our multi-tenant cloud.
Multi-Cloud Runtime	Boomi hosts and manages design time data in our multi-tenant cloud. The customer or our dedicated Managed Cloud Services (MCS) hosts the location, implementation and management of the runtime data.

Task Automation

Boomi Task Automation automates repetitive tasks with no code by connecting applications with pre-built templates to complete tasks. Applications are securely authenticated using OAuth Authorization. Task Automations can be enhanced according to industry best practices using Boomi Pathfinder (as discussed in Boomi AI above) and results can be tracked showing value adds in productivity.

Boomi DataHub

Overview

Boomi DataHub is a cloud-native data management platform solution that sits at the center of our customers' various data silos– including their existing master data management solutions, to provide an easy-to-implement, scalable, flexible, and secure data quality as a service.

Boomi's public Hub Clouds store data and offer robust security features that address data sovereignty concerns. Customers may choose the region where their data resides including as identified here. Customer data is encrypted in transit and at rest and enables Granular role-based access control with field masking options ensures only authorized users see specific data points.

DataHub Solution Architecture

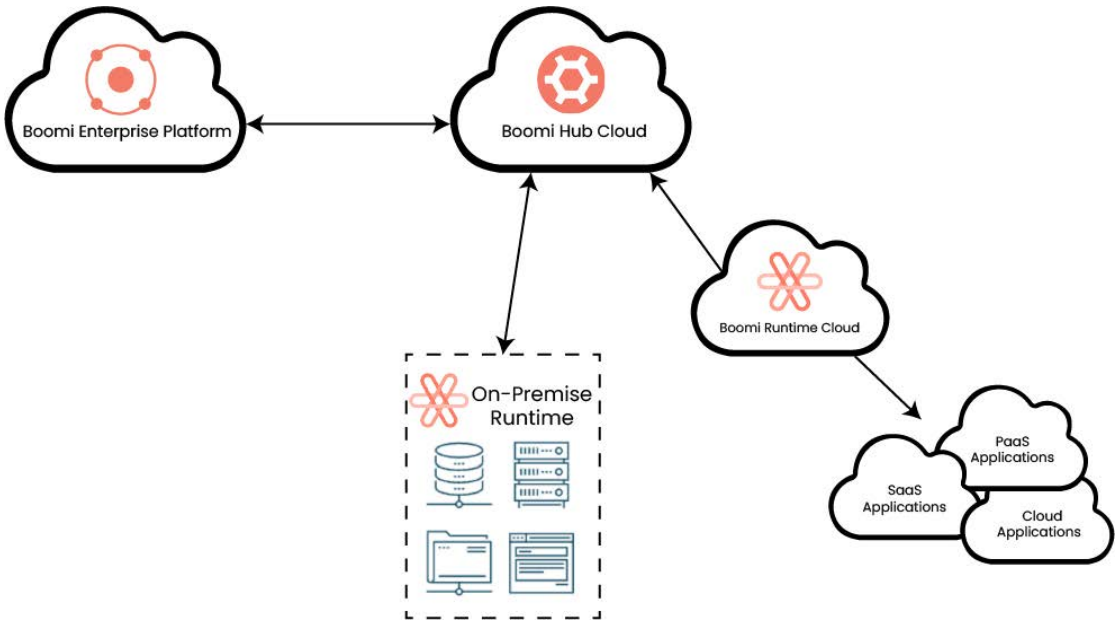

Diagram 18 - Hub Architecture

Data Path with DataHub

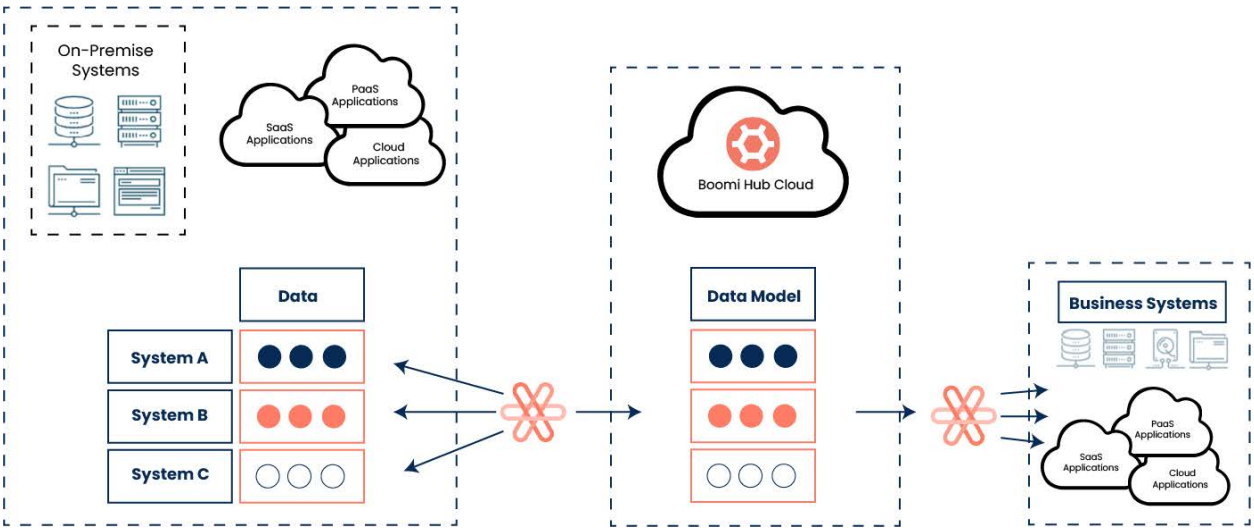

Diagram 19 – Hub Data Flow

DataHub Regional Repository Architecture

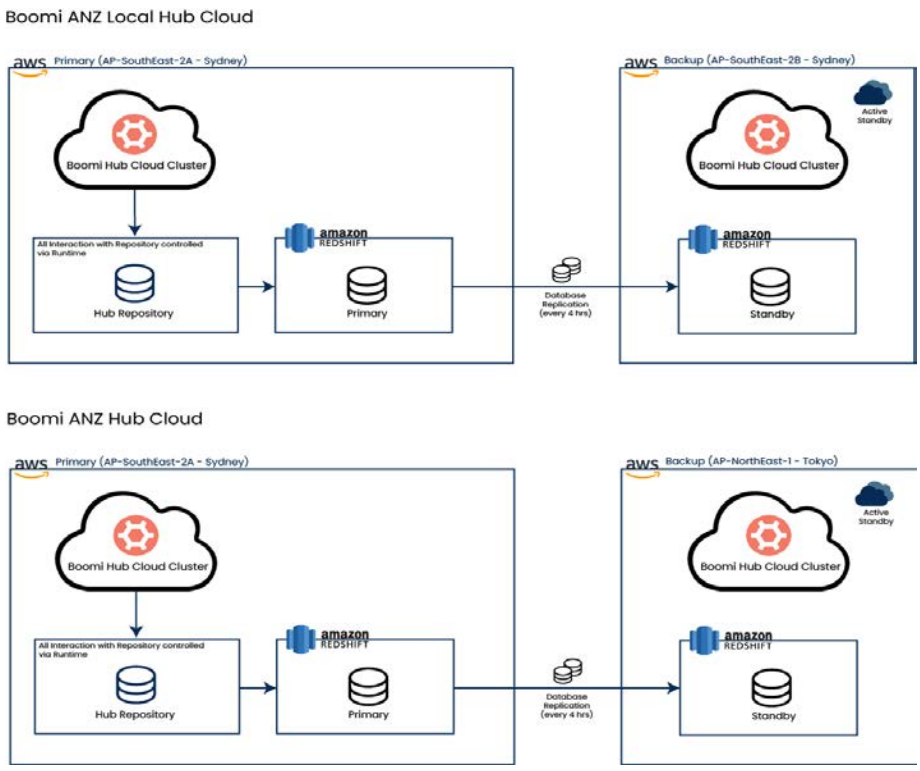

Diagram 20 – Hub Regional Repository Architecture Example

Understanding the Data Types

At Boomi, we delineate between data managed directly by the Boomi Enterprise Platform and data that resides within customer-controlled repositories in our regional public Hub Clouds. This distinction is important for understanding data ownership, control, and persistence. Elements such as historical reports, dashboard data, audit logs, repository configuration metadata, platform account data, and golden record field statistics (currently in Tech Preview) are managed at the platform level. This also includes the temporary data purging schedule, which is a platform-controlled function defining the automated retention periods for certain transient data. In contrast, other data types including source entities, transactions, activity reports, golden records, staged entities, quarantined entries, and bulk processing requests are repository-managed. This grants customers full control over their lifecycle and location within their chosen regional Hub Cloud, while still adhering to the defined platform-level purging schedules for associated temporary data.

The following table outlines the different types of data Boomi considers as part of the Boomi DataHub service.

Data Type	Description
Temporary Data Purging Schedule	For repositories hosted on a Boomi Hub Cloud, temporary data is purged on a defined schedule set out here. This process automatically removes transient data after a specified period to manage storage and ensure data lifecycle compliance. **Key Considerations:** This schedule dictates the persistence of temporary data within Boomi DataHub. Understanding these retention periods is crucial for data governance and compliance, as various data types are not retained indefinitely and are subject to automated deletion.
Source Entities and Batch Details	Original data records provided by external source systems for incorporation into a Boomi DataHub domain. This also refers to the specific information and metadata captured during the processing of incoming batches and individual entities, including details about the batch itself, such as processing completion, and granular information about each entity within the batch. **Key Considerations:** Their quality and format directly influence the master data. Source entities undergo validation, enrichment, and matching within DataHub. Batch and entity details are purged on a defined schedule after the completion of batch processing. This retention period is important for short-term troubleshooting and auditing of recent data ingestion activities.
Transactions	Processing events within the Boomi DataHub system that involve the validation, enrichment, incorporation, or

	quarantine of an incoming source entity record against existing golden records in the repository. **Key Considerations:** The retention of transaction details varies. Transactions not resulting in an operation on a golden record are purged on a defined schedule after the transaction's end. However, transactions resulting in the creation, updating, or end-dating of a golden record are retained on a defined schedule after the transaction's end. This differentiated retention policy reflects the varying long-term importance of transaction records for auditing golden record changes.
Activity Reporting (Inbound / Outbound)	Detailed logs providing a summary of data processing activities as data flows into (Inbound) and out of (Outbound) Boomi DataHub. This includes batch status, entity counts, transaction specifics, and information pertaining to the delivery of data, particularly outbound update requests from DataHub to source systems, including acknowledgments of successful deliveries. **Key Considerations:** Offers comprehensive audit trails for data movement. Essential for troubleshooting data flow issues, monitoring integration health, and verifying data synchronization with connected systems.
Historical Reporting	Aggregated and trend-based data reports that provide insights into the long-term performance and evolution of master data. This includes historical counts of golden records, quarantine trends, and data quality over configurable periods. **Key Considerations:** Supports long-term data governance strategies and historical auditing. Critical for performance

	analysis and identifying patterns or anomalies in master data changes over time.
Dashboard Data	Aggregated and visual summaries of key operational metrics and data health indicators within DataHub. This data is presented through various reporting interfaces for quick and actionable insights into data management processes. **Key Considerations:** Provides real-time and summary insights for operational monitoring and tracking. Enables quick identification of areas requiring attention, such as processing backlogs or high quarantine rates.
Golden Records	The authoritative, reconciled, and trusted version of a data entity (e.g., customer, product) established and maintained within a Boomi DataHub domain. **Key Considerations:** Represents the single source of truth for master data. Subject to stringent data quality, matching, and stewardship processes to ensure accuracy and consistency across the enterprise.
End-Dated Golden Records	Golden records that have been logically retired, marked as inactive, or moved to a historical state within a DataHub domain. These records retain their historical context but are no longer actively used for new operations. **Key Considerations:** Essential for maintaining historical data integrity and compliance with data retention policies. Allows for auditing of past relationships and data states without permanent deletion.
Staged Entities	Incoming source entities can be temporarily held in a "staging area" for preview, testing, and validation. These entities are

	processed to simulate incorporation but are not committed to the golden record domain until explicitly approved. **Key Considerations:** Facilitates controlled data onboarding, allowing for pre-validation of data quality and impact analysis without affecting live master data. Critical for testing new integrations or large data loads.
Reference Data	Within Boomi DataHub, "Reference Data" can also refer to the concept of **domain references**, where fields within one master data model (domain) establish a relationship or link to golden records in another master data model. This enables the enforcement of referential integrity across different data entities. **Key Considerations:** The persistence of these established relationships between golden records across different domains is fundamental to maintaining a holistic and consistent master data landscape. These references are an integral part of the golden record's definition and contribute to the overall data integrity and referential accuracy within the DataHub system.
Audit Logs (including Export activities)	Record of user actions, system events, and operational responses within the DataHub service. This includes detailed information on administrative changes, data modifications, and golden record export activities. **Key Considerations:** Provides a comprehensive, unalterable trail for security auditing, compliance, troubleshooting, and accountability. Essential for demonstrating adherence to data governance policies and regulatory requirements. Please note that audit log entries are retained indefinitely.
Quarantined Entries	Incoming source entities that failed to be incorporated into a DataHub domain due to validation errors, matching

	discrepancies, or other configured rules. These entries are held for manual review and resolution by data stewards. **Key Considerations:** Highlights data quality issues at the point of ingestion. Requires timely data stewardship intervention to prevent data loss or inconsistency. Critical for maintaining master data integrity. Resolved quarantine entries (except where superseded) are purged on a defined schedule after resolution, while superseded quarantine entries are purged on a defined schedule after resolution.
Bulk Processing Requests	Records detailing large-scale operations applied to golden records, such as mass end-dating, purging, or propagating updates to source systems. The status and details of these operations are tracked. **Key Considerations:** Provides a mechanism for managing and auditing high-volume master data changes. Ensures traceability and status visibility for significant data manipulation activities, supporting large-scale data governance. Bulk processing requests are purged on a defined schedule after creation.
Repository Configuration Metadata	Defines the structure, rules, and configurations of your master data models (domains) within DataHub repositories. This includes field definitions, match rules, data quality steps, and metadata related to integration processes. **Key Considerations:** Crucial for defining the integrity and behavior of master data. Includes configuration details related to how data is governed and processed within the platform.

Viewing Golden Record Field Statistics (Tech Preview)	Aggregated statistical insights into the characteristics and quality of golden record field values within a deployed DataHub model, derived from a sample of data. This feature helps assess data quality and troubleshoot issues. **Key Considerations:** A Tech Preview feature for proactive data quality assessment and model refinement.

DataHub Command Center

Boomi Command Center, powered by ServiceNow, extends Boomi DataHub's capabilities by providing tools for data visibility, traceability, and analysis. It offers a centralized view of master data for operational monitoring and oversight.

The Command Center integrates directly with customer DataHub repositories to provide information on how various data types are managed and evolve.

- **Dynamic Visualization:** Provides interactive, real-time representations of golden record business data and supporting metadata.
- **Source Linkage and Historical Metadata Analysis:** Tracks the origins and transformations of data, linking core data types such as source entities, golden records, and domain references to their original sources and recording subsequent changes. This feature also analyzes the historical context and evolution of data, including changes in data values, usage, and processing over time within DataHub. This combined capability provides a record of modifications, aiding in data provenance verification and correlation with audit logs for auditability, and supports the retrospective analysis of data handling practices and data quality trends.

Boomi Command Center delivers insights into data, its changes, and its sources. This visibility supports data governance, data quality monitoring, and security posture management.

Boomi Event Streams

Overview

Event Streams is a multi-tenant, enterprise message, queueing and streaming service fully hosted and managed within the Boomi Enterprise Platform. It supports common enterprise messaging patterns, like pub/sub and queuing, with guaranteed message delivery, ordering and availability. In combination with Boomi Integration, it provides a highly scalable and reliable backbone for an "event driven integration" approach.

Features

Feature	Description
Boomi Integration Connectivity	With the Event Streams connector, users can send and receive messages from Boomi Integration processes running on-premises or in the cloud.
Advanced Messaging Functionality	Event Streams offers several options for reliable message delivery, including FIFO with guaranteed ordering, pub/sub (fan out) for delivering the same message to multiple consumers, and queueing for high throughput use cases where ordering is not required.
Administration and Monitoring	Event Streams displays usage statistics for monitoring and observability purposes directly within the Boomi Enterprise Platform UI.
Token Management	Event Streams manages tokens used for authorization during data transmissions to support secure authentication. This ensures that only authorized systems can publish or consume messages through the event broker.
Message Management	Event Streams empowers users to efficiently handle all subscription messages in a centralized location. It allows for viewing the subscription backlog, downloading specific messages along with their metadata, bulk deletion of individual or multiple messages, and monitoring dead letter backlogs to ensure seamless event stream operations.
REST API Connection	Event Streams facilitates seamless integration via REST API connections, allowing external applications to produce and consume messages. This connection method supports easy integration with various data sources and applications.

Event Streams Architecture

The Event Streams Architecture consists of two primary components:

1) **Customer System:** Users establish connectivity with our Platform and configure a Boomi runtime. This Boomi runtime can be situated in their private cloud, on-premises, or within Boomi's cloud infrastructure. Customers utilize the Event Streams connector to produce, consume, and monitor messages in their workflows.
2) **Event Streams Admin UI and Event Streams Cloud:** Our Boomi Event Streams cloud encompasses the Event Streams Admin UI (hosted on AWS US East region). This interface monitors activities and facilitates tasks such as environment, topic, and subscription management. Messages exchanged through Event Streams connectors in various processes are orchestrated within the Event Streams cloud (hosted on AWS USA East, ANZ, UK and EMEA region).

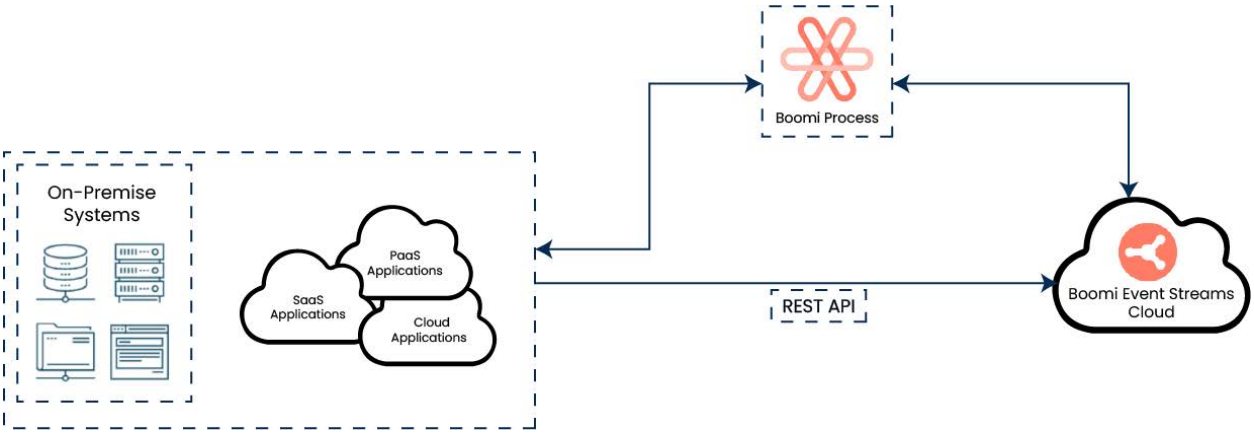

Diagram 21 – Event Streams Architecture

The Event Streams cloud is hosted in the US East, ANZ, EMEA, and UK Regions.

Data Flow

The interaction between the Boomi Event Streams cloud and the Boomi Platform occurs through three distinct processes: Produce, Consume, and Listen. The following diagram illustrates the general data flow within these scenarios.

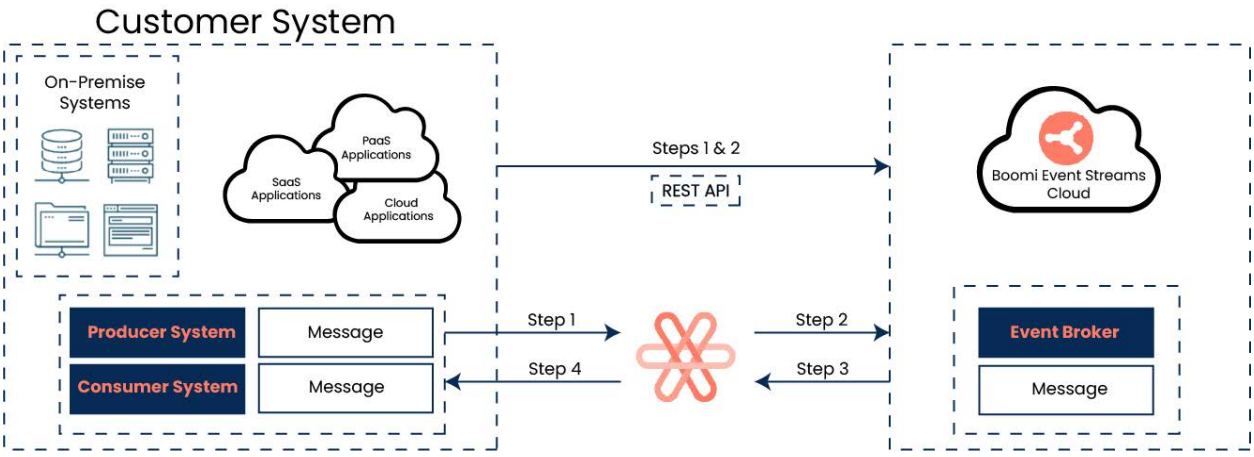

Diagram 22 – Event Streams Data Flow

The data flow involves four key steps:

Step 1 - Process Construction (Produce): The user constructs a process within our Platform, incorporating a producer connector, an Event Streams connector configured with the Produce action, and a designated Topic.

Step 2 - Data Transmission (Produce): Upon process execution, data/messages originating from the producer system are transmitted to the Event Streams cloud. In this cloud environment, the data is persisted within the event broker, sorted under the relevant Topic.

Steps 1 & 2 - Data Construction & Transmission (through REST API): In this method, data/messages are constructed within the customer's system and sent directly to the Event Streams cloud using the REST protocol. The transmission includes an authorization bearer token for secure access. Upon reaching the Event Streams cloud, the data is persisted within the event broker under the designated Topic.

Step 3 - Process Creation (Consume/Listen): A new process is crafted within our Platform, equipped with an Event Streams connector featuring either a Listen or Consume action. This process also includes a specific subscription linked to a Topic.

Step 4 - Data Retrieval and Processing (Consume/Listen): Upon execution of the new process, data/messages are retrieved from the event broker residing within the Boomi Event Streams cloud. Subsequently, these messages undergo consumption and processing as dictated by the process configuration.

There is one distinct data type related to Event Streams processes:

Name	Description
Event Streams Message Data	In addition to the processed data, messages exchanged via the Event Streams connector are securely transmitted to and from our Event Streams cloud. This secure transit is ensured through TLS encryption and is further safeguarded by encryption within the event broker's storage when at-rest. Security is reinforced by the utilization of a JSON web token (JWT), enabling secure and confidential communication among internal services. Messages destined for Event Streams are durably stored across multiple nodes, ensuring high availability, until they are acknowledged by consumers. To maintain efficiency and cleanliness, messages not acknowledged within 15 days are automatically purged from the system.

Data Boundaries

Event Streams, encompassing both the Admin UI and Event Cluster components, are deployed within regional datacenters. All data, including that of the Admin UI and Event Cluster, remains exclusively within these regional boundaries and is not replicated beyond those borders.

Viewing Data with Boomi Customer Support

Overview

Boomi operates a 24-7 “follow-the-sun” support model. So, depending on the issue, and the time of a raised ticket, a customer may be assisted by a Boomi employee located in various parts of the world. Boomi support teams operate in the US, Canada, Ireland, UK, India and Australia. Further details on Boomi Support are set out in the documentation available at help.boomi.com.

Boomi utilizes third-party SaaS technology to administer its support services, as set out at www.boomi.com/legal/sub-processors.

Boomi has conducted a Transfer Impact Assessment (TIA) on these transfers. For a copy of such TIA please reach out to your Boomi account team.

View Data

View Data is a user role inside of the Platform which allows users to view process logs and/or underlying Processed Data.

This out-of-the-box functionality allows Boomi customers to customize who can view (and not view) results or Processed Data.

When using this functionality, the Processed Data (upon request) is audit logged and transmitted from the runtime DB (encrypted in transit) through the Platform (where it is decrypted, cached), where it can be temporarily viewed by the user. The user controls the relevant purge / deletion of this data.

Every View Data request triggers a new process that extracts the data from the runtime DB to be viewed by the user via the Boomi Platform. The Boomi default setting on deletion on cached data is, at most, 30 minutes. However, users can update their preferences for deletion to be immediate upon closing the session.

Boomi automatically enables this privilege on all customer accounts; however, this function can be disabled by the customer's account administrator. This administrator limitation is in the "Test Mode" as well.

View Data with Boomi Customer Support

Customer account administrators control the roles and access privileges. Customers may limit the scope and use of the View Data feature by their own team and Boomi's support team.

Boomi utilizes a global CRM tool, and details shared with Boomi as part of user support cases, will be stored in the CRM tool. This tool is hosted in the US and accessed globally as part of the Boomi support process.

The transmission of data through the Boomi Enterprise Platform is subject to Supplemental Measures, as set out in the Boomi DPA.