

LUZmo

Security at Luzmo

January 2024

Table of contents

Introduction	1
Our services	2
Architecture	3
Security in depth	5
Physical security	5
Organizational security	6
Network security	7
Data security	8
Application security	8
Data Locality	8
Access Rights Model	10
Integration with multi-tenant platforms	12
Integration with single-tenant platforms	13
Privacy & Data Confidentiality	13
Incident Response & Management	14
Attestation & compliance	15
Contact us	16

Introduction

This whitepaper is intended to give you a clear & thorough insight into the steps taken by Luzmo to safeguard your data and reduce the risks of processing or storing data in our platform.

Specifically, we give an overview of our layered approach to security, with appropriate policies & controls at both organizational, physical, network and application levels.

Document version: January 2024



Our services

Luzmo delivers a cloud-based low/no-code web platform that enables SaaS or software suppliers to **seamlessly integrate data visualization & analytics** functionality into their products. Luzmo consists of a state-of-the-art interactive dashboard editor to craft bespoke dashboards or templates, a backend capable of lifting large data workloads and fully open APIs to automate or script just about anything happening in our platform.

Luzmo's team of 50 serves 220+ customers in 36 countries, including clients like BNY Mellon, WorkMarket (ADP Group), Selligent and government agencies like the Belgian Public Services of External Affairs and Economy.

Unique capabilities include an **API-first** design, full support for **multi-, single- or hybrid-tenancy**, including **advanced parameterization & theming** to personalize the experience for each end-user, strong support for **responsive multi-device** dashboards and multi-linguism and **data-driven actions** to transform dashboards from just a reporting tool to interactive UI components.

The image shows a dashboard for 'Awesome SaaS Company' with several callout boxes highlighting key features:

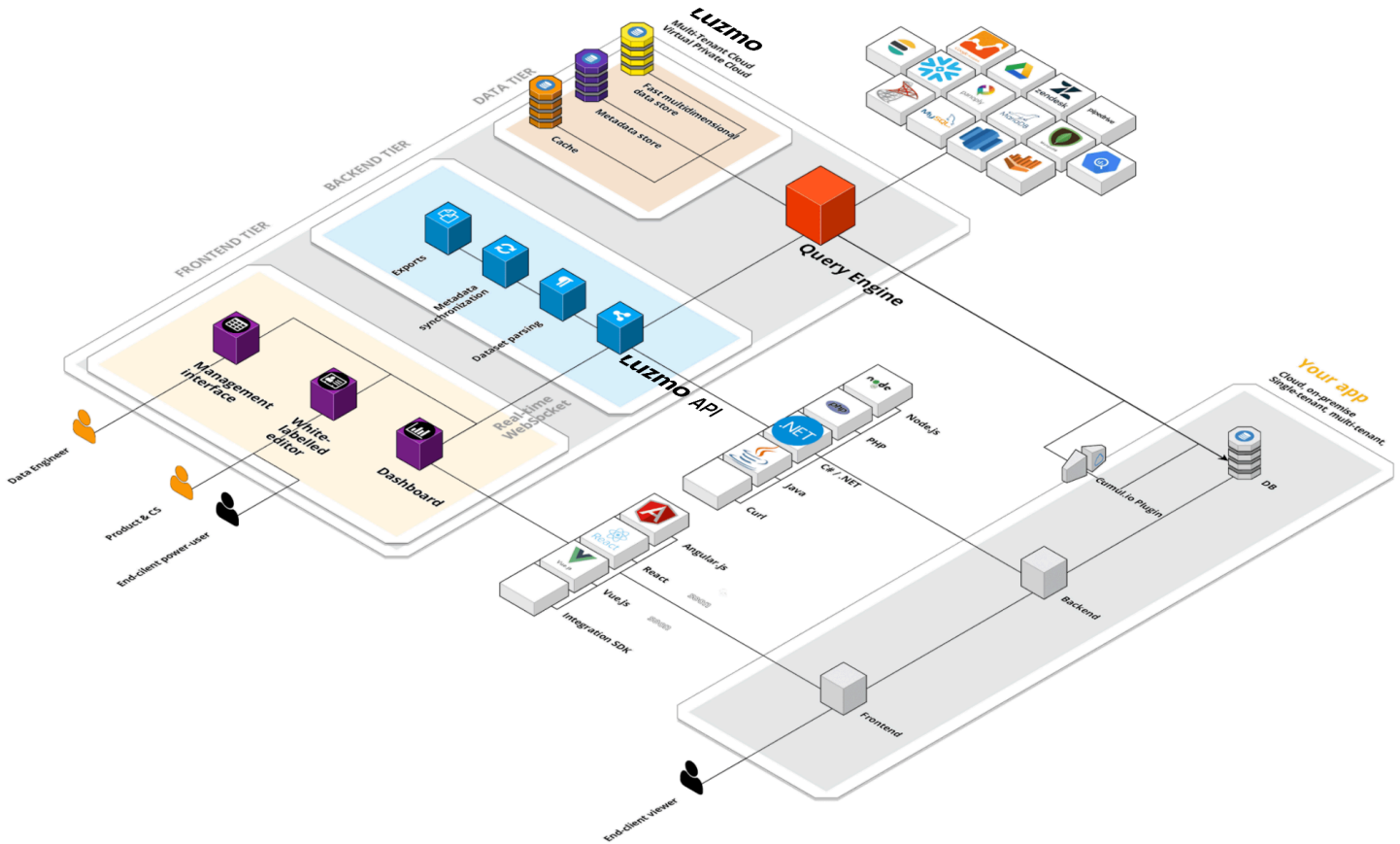
- Seamlessly embed:** Style dashboards to seamlessly fit your own application.
- API first:** Use user selections or context to programmatically create on-the-fly dashboards using our powerful API! (Callout points to a 'Generate Insights' button).
- Multi-lingual by default:** One dashboard can handle multiple languages. *C'est chouette n'est-ce pas?* (Callout points to a language dropdown menu).
- Multi-tenant out of the box:** Securely embed. Only show the data your end user is allowed to see. Filter data based on user, roles and even context! (Callout points to a user profile picture).
- Data Driven Actions:** Let your platform interact with the embedded dashboard. Retrieve data or filters from the dashboard and make that data actionable. (Callout points to a 'Resolve selection' button).

The dashboard itself displays various metrics and charts, including:

- Total Construction Spend: \$7.7M
- 95% of total budget spent
- 35% Client Satisfaction
- Average time to resolve incident per supplier (in days)
- Distribution per type of defect
- Reasons for rejecting quality inspection
- Number of quality inspections passed

Architecture

The Luzmo architecture has been designed to be fast, flexible and as secure by design as possible:



- Frontend:** includes management interfaces for creating and managing new data sources, datasets and intuitive drag-and-drop interface to craft new dashboards and data visualizations. The visualizations can be securely embedded in other platforms using Luzmo's Integration SDKs: WebComponent, Angular, React, React Native, Vue.

- **Backend:**
 - API tier with REST/Websocket APIs to interact with data sources, datasets, dashboards and other entities in the Luzmo Platform. The API is fully documented and open for Luzmo's customers to automate tasks or integrate with their own platforms.
 - Worker tier for IO or computationally intensive workloads, including parsing of unstructured datasets, creation of thumbnails or dashboard exports, live alerting, ... These are handled by pools of worker services.
- **Query Engine:** responsible for real-time execution of complex, multi-dimensional analytical queries over disparate connected data sources, using statistical optimization techniques to maximize performance and throughput.
- **Storage tier (optional):**
 - Cache: intermediate query result caching that can be enabled optionally.
 - Multi-dimensional data store: a fast data store optimized for analytical queries (ie. queries that typically hit a large portion of the historical & live data and use grouping & aggregation).
- **Data Connectors:** real-time data connectors to various relational database systems (including PostgreSQL, MySQL, SQL Server, MariaDB, Oracle), data warehousing platforms (Redshift, Snowflake), NoSQL data stores (MongoDB, Elasticsearch), web services (Google Drive, Google Analytics, Salesforce), etc. Customers can also craft their own bespoke connector via the open Luzmo Plugin API specification.

Security in depth

Luzmo has set up a comprehensive program of policies and procedures to set and maintain a high level of security throughout its organization. The main objectives include:

1. Reduced risk of data breaches
2. Safeguarding of client's data or data entrusted by clients to us for processing or storage
3. Compliance with legal, regulatory, and contractual requirements, incl. GDPR and CCPA

Physical security

Luzmo commits to contracting exclusively ISO 27001-certified data centers that pass our vendor assessments, which include physical entry, security and monitoring requirements.

Our server infrastructure is currently operated by:

- Amazon Web Services EMEA SARL
- Hetzner Online GmbH

Luzmo offices are treated as a secured zone as well, and workstations and devices used by employees must adhere to our Workstation Policy.

Organizational security

Luzmo has put in place a strict framework of organizational policies & processes. Among others, all new employees are onboarded using our Access Onboarding & Termination Policy (AOTP). Employees are trained depending on their position in the company, following our Policy Training Policy (PTP) and must adhere to a Code of Conduct.

All staff at Luzmo are regularly trained in Security Awareness, including recognizing social engineering attacks, secure password management, handling of confidential data, compliance, etc.

Our management team is fully committed to security: they regularly review incidents, monitor the threat landscape and update policies accordingly. Security policy is discussed in Executive Management meetings and within the Board of Directors.

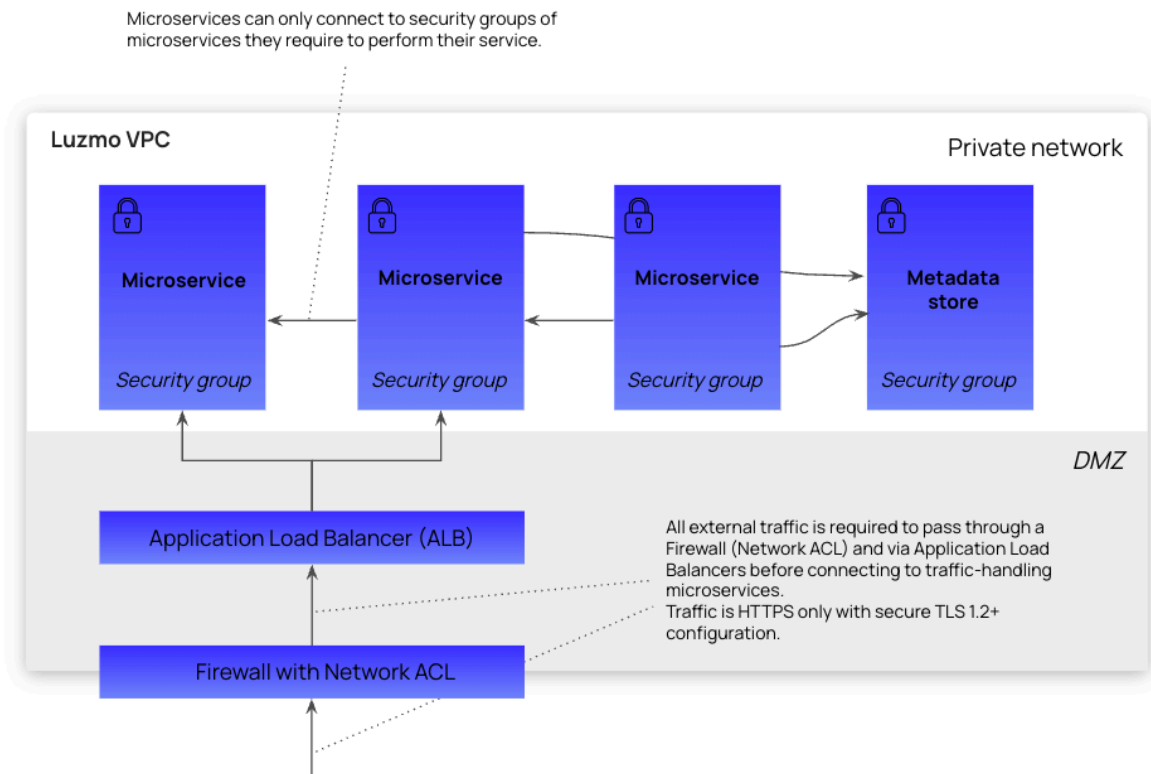
Access to the code version control system, build & deployment environment, server infrastructure, data & backups and other assets are strictly controlled & audited:

- Only technical personnel have access to the code version control system. All code & configuration changes are reviewed (multiple eyes principle) and tested using manual acceptance testing and suites of automated unit tests, integration tests and end-to-end frontend regression tests.

- Change sets are never manually executed, but only run through repeatable, reversible & automated Continuous Integration & Continuous Deployment (CI/CD) pipelines.
- Access to the CI/CD & production infrastructure is restricted to key personnel of our Operations team and strictly limited to the duration of the intervention requiring the access only. Two-factor authentication is mandatory on all development & production systems. All accesses to systems are logged & regularly audited.
 - **Production level:** access to CI/CD & production infrastructure, **no access** to production customer data.
 - **Production Data level:** access to production customer data, for resolving critical production incidents only.



Network security

Luzmo runs its platform as container-based workloads on an auto-scaling fleet of servers running on hardened “golden” machine images that are kept up-to-date by our Operations team.



We use “defense-in-depth” techniques: different environments are shielded in fully separated Virtual Private Clouds with Network Access Control Lists. Microservices are placed in separate Security Groups to ensure they can only reach other services they depend on and can only be

reached by other services that need them. All external traffic is proxied through secured load balancers.

Network connections are secured using TLS v1.2+ connections. Our TLS configuration has an [A+ rating](#)  according to [SSL Labs](#) .

Data security

Metadata, data and credentials stored & processed on the Luzmo platform are encrypted both in storage and in transit. Data is only decrypted when processed (eg. application of aggregations, group by-operators, filters, ... in the Query Engine).

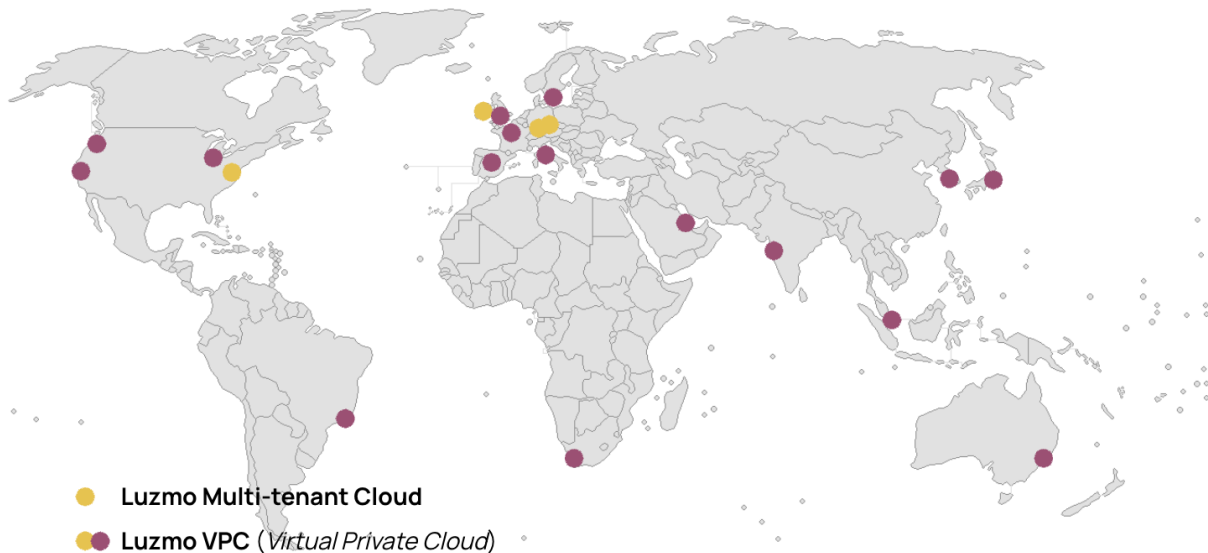
Credentials are salted, peppered & hashed before storage. Encryption keys are managed in a Hardware Security Module (HSM). All encryption keys and secrets have minimum complexity & length requirements and are rotated on a regular basis.

Application security

Secure application design is considered and tracked starting from the Requirements Analysis phase over Architecture & Design to secure Development, Testing, Deployment, Operations & Maintenance and Decommissioning phases, per our Software Development Lifecycle Policy (SDLCP).

- Applications are developed according to our Application Security Policy guidelines. These include proper classification of data confidentiality levels, input validation guidelines, testing standards, required security self-assessments (including OWASP Testing Guide, OWASP Top 10 quick scans, ...).
- Automated vulnerability scanning & dependency analysis is used. The platform is also pen-tested regularly by external parties.
- We follow NIST SP 800-63-3 standards on Digital Identity management and SP 800-175B standards on use of Cryptographic Standards.
- All developers are trained in secure application design. Change sets are reviewed and explicitly vetted for secure code practices. Incidents are discussed with everyone involved and procedures improved iteratively.

Data Locality



Luzmo Multi-tenant Cloud (default):

Luzmo operates a multi-tenant cloud that automatically scales in response to predicted & actual load on our platform. Customer organizations are segregated logically.

- Customers choose their data tenancy (EU or US) on creation of their organization. We make sure data is exclusively stored & processed within data centers located within your chosen jurisdiction.

We currently make use of data centers in Ireland (Dublin area), USA (Ohio region) and Germany (Frankfurt & Nuremberg areas) by Amazon Web Services EMEA SARL and Hetzner Online GmbH.

- By default, we *do not* store your data on our platform. In this case, data is only flowing through and processed by our systems.

Data is stored in Luzmo only if you make use of any of the following data connectors:

1. Local file upload (Excel, CSV, JSON, ...)
2. API push (see [Developer portal](#))
3. Web service connectors (Google Drive, Google Analytics, ...)

Data is temporarily cached in memory only if you optionally enable dataset caching for a particular dataset. You are in control of the maximum time-to-live (TTL) of this cache.

- Luzmo will never independently initiate a transfer of data out of your chosen jurisdiction.

Note that you or your customers might access dashboards outside of your jurisdiction, eg. via Private Share URL, by logging in while on-the-go, ... This might legally constitute a cross-border transfer of Personally Identifiable Information, if you are processing such data.

In case of data transfer outside of the EU, we make use of Standard Contractual Clauses to guarantee it is safeguarded to the same standards as when stored in the EU.

Luzmo Virtual Private Cloud (optional):

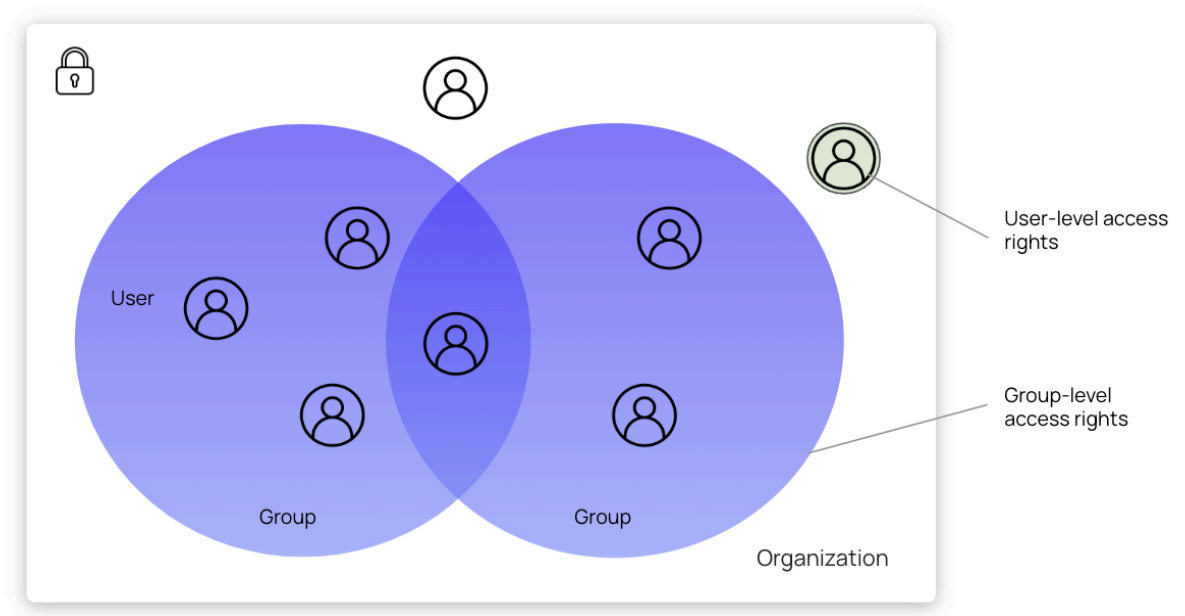
Our Virtual Private Cloud offering, which offers you a fully managed but dedicated Luzmo stack, is **launched in one or more AWS regions of your choice**.

- For VPCs within the European Union, we make sure data is only stored & processed within the European Union.
- Within a VPC, it is possible to set-up VPC Peering or VPC Endpoint Services to setup secure data connections to data sources within your own AWS account, without traffic ever leaving the private network.
- A VPC optionally follows a Long Term Stable (LTS) release of the Luzmo platform, which receives monthly updates instead of the multiple daily release cycle of the Multi-tenant Cloud.

Access Rights Model

Luzmo contains an extensive & flexible access rights model:

Entity	Description
Organization	Organizations are secure enclaves within Luzmo. Data sharing within Luzmo is only possible <i>within</i> an organization ¹ . Each user is part of a single organization.
Groups	Groups of users with similar access rights or roles. Each user can be part of multiple groups. Datasets & dashboards can be shared at the group and/or user level. This enables you to create multi-level access right controls.
Users	A named user within the Luzmo platform with its own credentials. This can be either an organization Owner (who can set organization policies and manage users & groups), a Designer (who can manage data connections, datasets and design dashboards) or a Viewer (a user who has read-only access to dashboards, in a clean portal environment).



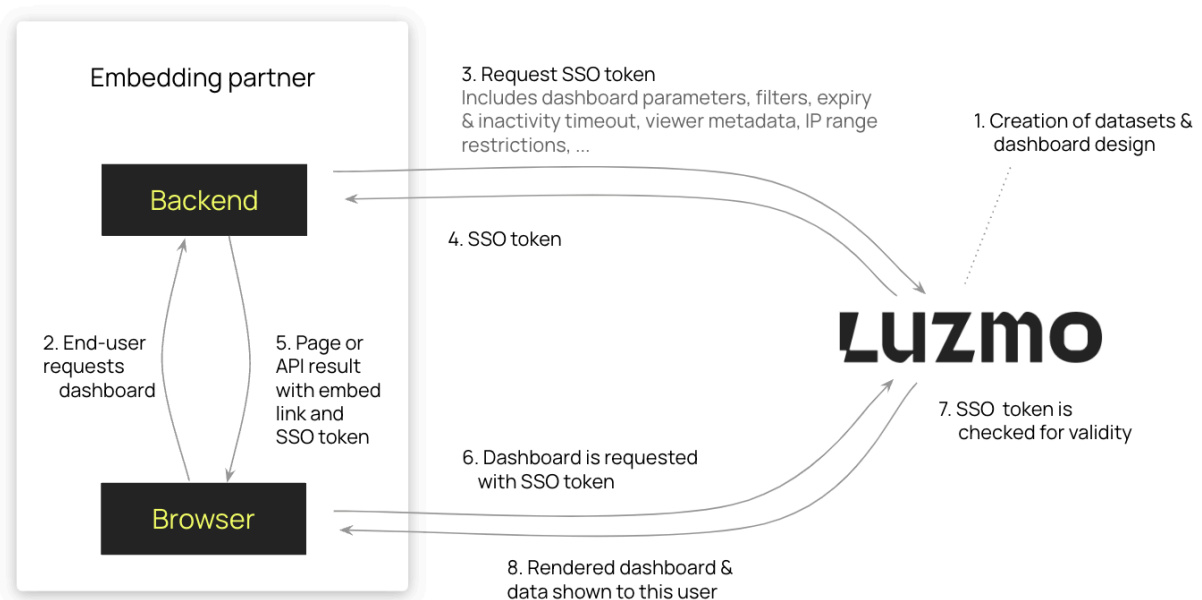
Access rights for Users & Groups can include:

- **Read-level access:** ability to retrieve data from a dataset

¹ With the exception of *Private URL Shares*: this is a way to link to Luzmo dashboards via a unique URL without requiring further authentication. This functionality can be disabled for an organization.

- **Use-level access:** ability to use a dataset as a source in a dashboard
- **Modify-level access:** ability to adapt derived columns or data types of a set, or adapt a dashboard
- **Own-level access:** ability to set access rights & share the dataset or dashboard
- In all cases, access can be limited on a row-by-row basis (“row-level security”), eg. only data of a particular (set of) customer(s), country, ... or any other filter that can be applied to one or more columns of a dataset.

For secure integration & embedding within other platforms, Luzmo enables you to create **disposable authorization tokens** that delegate access to one or more datasets and dashboards and can personalize a dashboard’s experience, in row-level security filters, dashboard parameters, dashboard styling & theming, etc.



Integration with **multi-tenant** platforms

To integrate with a multi-tenant platform, ie. where data for each end-customer is stored in a single data store and segregated logically, you can set **parameter filters** within your dashboards. You then set the parameter values for a particular end-user in the disposable authorization token:

```
client.create("authorization", {
  type: "sso",
  ...
  expiry: "1 hour",
  metadata: {
    client_id: [1337],
    country_id: 'US'
  }
})
```

During each step of the data flow, Luzmo guarantees that your filters are applied. If you are using Luzmo Plugins, we even send the metadata your way, so you can call user-specific code in your plugin or re-use your existing business logic. You can also securely transport your own API token through a disposable token to call your API on your end-user's behalf.

Integration with **single-tenant** platforms

To integrate with a system in which you have a separate database, set of tables, schema, shard, server or even datacenter per customer, you can use **account overrides** to instruct Luzmo to dynamically connect to a different environment, ... within a single dashboard:

```
client.create("authorization", {
  type: "sso",
  ...
  expiry: "1 hour",
  account_overrides: {
    <your connection ID>: {
      host: 'client1.unitedburrito.com',
      schema: 'client1',
      identifier: 'client1',
      token: '*****'
    }
  }
})
```

There are a variety of ways to combine built-in security primitives, tokens, parameters & account overrides for hybrid-tenant platforms. Our Solution Engineering team is committed to help you find an optimal way of arranging our tools.



Learn more about multi-tenancy: [How to handle multi-tenancy in Luzmo](#)

Privacy & Data Confidentiality

Luzmo complies with global data protection & privacy regulations, including GDPR (General Data Protection Regulation) and CCPA (California Customer Privacy Act).



Luzmo acts as a **Data Controller** for the following types of data:

- Data on our customers, including email addresses and business contact information
- Visitor engagement data, including IP addresses

We only collect & use Personally Identifiable Information if we strictly need to to render our services. Data is handled securely and kept only as long as it is necessary. We have procedures in place to diligently & timely process GDPR notices with regards to the rights to access, rectification, erasure and data portability.

Luzmo acts as a **Data Processor** for the following types of data:

- Data stored or processed on the Luzmo platform, which may include Personally Identifiable Information, potentially in special treatment categories.

Customers can sign a Data Processing Agreement as an addendum to the Terms & Conditions within our Legal & Compliance portal. It further details our duties & diligence as a data processor and the steps we take in case of accidental loss of data.

Incident Response & Management

Luzmo has a strict Security Incident Response Policy (SIRP) in place to respond to identified vulnerabilities or security incidents. Ongoing incidents are managed by an Incident Coordinator, and are communicated via the [Luzmo Status](#) panel:

Incidents

None in last 30 days

In case this is warranted, ongoing or resolved incidents will also be communicated to the registered Data Protection Officer (DPO) or European Union Representative (EUR) of your Organization, or the Belgian Data Protection Agency (DPA).

You can register a DPO or EUR as an Organization Owner within Luzmo's Legal & Compliance portal.


Incidents are also reviewed periodically to sharpen operational security practices and employee training programs and improve our policies.

Attestation & compliance

Luzmo works with external parties to validate, improve test & certify our security practices & policies:

- Our internal processes, policies and controls are SOC2 compliant and are mapped to the Trust Service Criteria (TSC) framework. We hold a SOC2 Type 2 report, which is renewed annually and available upon request under NDA.



- We exclusively use ISO27001-certified data centers. Our primary data centers are operated by Amazon Web Services EMEA SARL. AWS is, among other certifications, fully SOC2-compliant. You can retrieve the full SOC2 report upon request.
- We regularly let our partner [nSEC/Resilience](#)  perform 3rd party penetration testing of our network and applications. The certificate and detailed pentesting results are available upon request.

Contact us

Still have questions related to security or our solutions? Feel free to contact us and we'll gladly help you out and design a solution on our platform that fits your needs.

EU Data Protection Officer

Haroen Vermylen
Martelarenlaan 38
3010 Leuven
Belgium
dpo@luzmo.com
+32 499 15 38 61
+1 (646) 783-4676

Support Team

support@luzmo.com

Sales Team

hello@luzmo.com

Solution Engineering Team

solutionengineering@luzmo.com

Luzmo HQ Europe

Luzmo NV
Martelarenlaan 38
3010 Leuven
Belgium

Luzmo HQ USA

Cumul.io, Inc.
77 Sands St - 9th floor - Office 9035
Brooklyn, NY 11201
United States